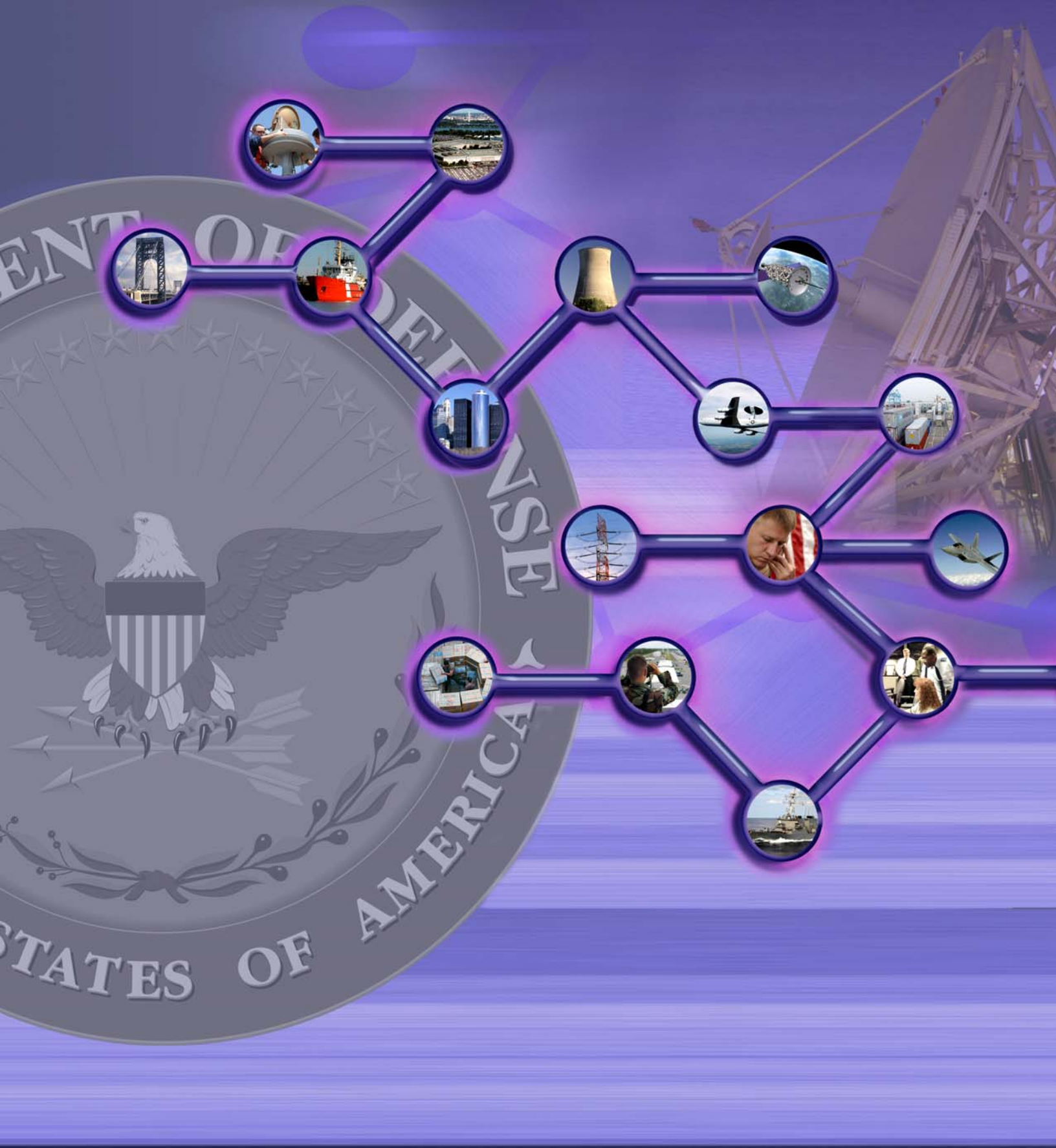

Department of Defense
Critical Infrastructure Protection

Developing a Comprehensive and Integrated Vulnerability Assessment Methodology for the Defense Department's Critical Infrastructure Protection (CIP) Program

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
12 DEC 2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Defense Critical Infrastructure Protection. Developing a Comprehensive and Integrated Vulnerability Assessment Methodology for the Defense Department's Critical Infrastructure Protection (CIP) Program	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Director for Critical Infrastructure Protection,Office Asst Sec of Defense fro Homeland Security,Washington,DC,20528**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**84**	

DEVELOPING A COMPREHENSIVE AND INTEGRATED VULNERABILITY ASSESSMENT METHODOLOGY FOR THE DEFENSE DEPARTMENT'S CRITICAL INFRASTRUCTURE PROTECTION (CIP) PROGRAM

A REPORT SUPPORTING CIP PROGRAM OUTREACH AND EDUCATION

Director for Critical Infrastructure Protection

Office of the Assistance Secretary of Defense for

Homeland Defense

12 DECEMBER 2003

EXECUTIVE SUMMARY

This report was prepared to support the Department of Defense (DoD) Critical Infrastructure Protection (CIP) strategy for Outreach, Education, and Training. It seeks to help those interested in understanding the Defense Department's current concepts and plans for developing CIP-specific vulnerability assessments. The report ties together and summarizes the many documents that were prepared from 1998 until 2003 and that cover assessment descriptions, applications, information sharing, and a range of other issues related to assessment methodology. Annex B provides a summary of the problems found and the solutions recommended in each of DoD's CIP vulnerability assessment studies beginning in 1999 and completing in 2003.

The report organized the material into five sections, with each section addressing one of a set of questions about the nature of the DoD vulnerability assessment concept and efforts made to develop a comprehensive and integrated assessment program.

What is the concept of Department of Defense (DoD) CIP vulnerability assessment? One way to understand the DoD CIP assessment concept is to understand the component elements within the policy definition for the term "vulnerability assessment." As defined within DoDI 3020 (Draft), it is "The process of determining the susceptibility of critical assets, associated infrastructures, or interdependency related single points of failure to adverse conditions." The DoD definition of vulnerability assessment requires the understanding of four concepts – asset susceptibility to adverse conditions, associated infrastructures dependencies, asset infrastructure interdependencies, and single points of failure. An earlier concept for vulnerability assessment was based on the original guidance from risk management practice as stated in the 1998 DoD CIP Plan and from the Critical Asset Assurance Program (CAAP). This guidance envisioned a program, which would determine critical assets that have known vulnerabilities combined with known threat exposure. From this analysis, the CAAP process would develop vulnerability metrics that base the remediation process on established and reliable criticality and vulnerability standards. However, the DoD CIP community could not agree as to the appropriate standards to transition the guidance from the CIP Plan and CAAP into an operational assessment process.

How does the vulnerability assessment process contribute to the DoD CIP program? The goal of CIP vulnerability assessments is to achieve greater fidelity of information for the senior DoD leadership and Combatant Commanders to use in assessing the risks to critical assets and, consequently, to military capabilities and operations. Vulnerability assessments are essential in identifying infrastructure asset vulnerabilities and generating remediation options. Under the DoD CIP strategy, a fundamental part of the CIP program requires conducting comprehensive and tailored CIP vulnerability assessments on both scenario-independent and scenario-dependent critical infrastructure assets only *after* identifying, validating, and prioritizing vulnerability assessment requirements. This way, DoD can preserve scarce vulnerability assessment resources and skills for the most important assets.

What are the characteristics of the vulnerability assessment methodologies commonly used in the DoD CIP program? Previous studies under the OASD (C3I) CIP Directorate identified 22 DoD vulnerability assessments that had CIP relevance and shared some

common characteristics. The four vulnerability assessment methodologies summarized in Section 3 (Integrated Assurance Program, Joint Staff Integrated Vulnerability Assessments, Balanced Survivability Assessment, and the Navy/Marine Corps Integrated Vulnerability Assessment) shared the most common characteristics.

1. The methodologies addressed several areas of critical CIP assessment interest: physical security, operations security, information security and assurance, support of commercial relationships, industrial security, safety, continuity of operations, and remediation recommendations. This wide range of assessment interests will eventually permit assessors to consider most of the environmental factors that affect a critical asset's ability to function properly to accomplish mission tasks.
2. The methodologies placed emphasis on specific standards derived from DoD and other Federal or related industry technical specifications and best practices. This experience indicates that anchoring an assessment process to specific standards makes the process a reliable, repeatable one that can provide consistent outcomes.
3. The methodologies included a set of assessment protocols to guide the assessment process: pre-assessment information exchange, onsite observations and interviews, a pre-established checklist for recording data, periodic assessment team back-briefs to the installation or facility commanders or managers, onsite exit briefing, and a final report delivered some 60 -120 days following the end of the assessment. Standardizing these protocols could lead to a process that, if centrally planned and coordinated, would logically and deliberately prioritize and schedule DoD-wide vulnerability assessments.
4. The methodologies provided the installation or facility commander with recommendations for remediation activities based on specific assessment findings. The feedback process not only addresses specific vulnerabilities, but also allowed for the exchange best practices within the DoD CIP community.

Is there a common basis for a standard DoD CIP vulnerability assessment process? The three major investigative activities conducted by the OASD (C3I) CIP Directorate from 1999 until 2003 generated numerous recommendations that influenced the current OASD (HD) proposal for a standardized DoD CIP vulnerability assessment methodology.

1. The Demonstration Projects (1999-2001) identified the necessity of a deliberate pre-assessment activity to synchronize the distinct protocols of several cooperating assessment methodologies within an assessment mix oriented on a given set of infrastructure assets supporting a given Combatant Command mission. While separately, the individual assessment methodologies have had their own specified pre-assessment requirements, the Demonstration Projects, particularly the RMC project, demonstrated the value in synchronizing the pre-assessment activities of each.
2. The joint PACOM and JPO-STC Appendix 16 Pilot Project (2002-2003) validated the pre-assessment findings from the Demonstration Projects and identified two major areas for assessment standardization. First, they demonstrated the effectiveness of tailoring specific assessment characteristics of the DTRA BSA and JSIVA, and the JPO-STC IAP assessment to the most appropriate mission critical assets. Second, they demonstrated the need to convert assessment report outputs into electronic data elements to link asset identity, characteristics, interdependencies, vulnerabilities, and

remediation options into a properly secure, but accessible site for mission planners, asset owners, and other interested CIP Component organizations.

3. The two OASD (C3I) vulnerability assessment study teams (2001-2003) verified that the current assessment process remains fundamentally uncoordinated, non-integrated, and redundant. Therefore, there remains requirements to establish of specific DoD policy for vulnerability assessments, create an integrated CIP assessment process that "leverages the best practices" of existing assessments, and establish information sharing processes with requisite levels of security classification.

What is the plan to develop a standardized DoD CIP vulnerability assessment process?
The proposed DPO-MA CIP vulnerability assessment program – Full Spectrum Vulnerability Assessment (FSVA) - will develop the policies and standards for a comprehensive DoD-wide approach for assessing critical infrastructure vulnerabilities. The program complements the DoD CIP analysis process to identify critical infrastructure assets. It aims to provide quantifiable measures to the DoD leadership and Combatant Commanders to enable them to judge the vulnerabilities of mission-essential critical assets and support the identification of the risks to military capabilities and operations. The fully developed DPO-MA CIP FSVA program would contain the following elements:

- Comprehensive DoD CIP assessment policy and associated program instruction
- DoD CIP FSVA Program management Plan
- Established, and periodically updated, DoD CIP FSVA standards and protocols
- DoD CIP FSVA training and certification program
- DoD CIP FSVA program User's Guide
- Database management process to record FSVA data to the DoD CIP asset database

In conclusion, the DPO-MA FSVA concept is a logical methodology that reflects the collective DoD CIP program experience in both conducting vulnerability assessments and analyzing the various assessment processes. The next step will be to refine the concept through a collaborative exchange with the various assessment stakeholders within the DoD CIP community to transition the concept into a supportable, DoD-wide, CIP vulnerability assessment program

TABLE OF CONTENTS

INTRODUCTION	**3**
SECTION 1 - DEFINING VULNERABILITY ASSESSMENT WITHIN A NATIONAL DEFENSE CONTEXT	**5**
SECTION 2 - THE CIP FUNCTION OF VULNERABILITY ASSESSMENTS	**13**
SECTION 3 – CHARACTERISTICS OF VULNERABILITY ASSESSMENTS COMMONLY USED FOR THE CIP PROGRAM	**21**
SECTION 4 – SEEKING A COMMON BASIS FOR A STANDARDIZED CIP VULNERABILITY ASSESSMENT	**36**
SECTION 5 – DOD ACTIVITIES LEADING TOWARD THE DEVELOPMENT OF A STANDARDIZED CIP VULNERABILITY ASSESSMENT	**51**
SUMMARY	**61**
ANNEX A – TABLE OF DOD VULNERABILITY ASSESSMENT METHODOLOGIES AS CITED IN THE JPO-STC VULNERABILITY ASSESSMENT CATALOG (2003)	**66**
ANNEX B – SUMMARY OF FINDINGS AND RECOMMENDATIONS FROM PREVIOUS DOD CIP VULNERABILITY ASSESSMENT STUDIES AND INVESTIGATIVE PROJECTS (1999-2003)	**70**
ANNEX C - VULNERABILITY ASSESSMENT ANNOTATED BIBILOGRAPHY	**74**

INTRODUCTION

Background. In its capacity as the CIP program office for the Office of the Assistant Secretary of Defense for Homeland Defense (OASD (HD)) CIP Directorate, the Defense Program Office for Mission Assurance (DPO-MA) developed the concept for a CIP vulnerability assessment process in October 2003. Their concept for vulnerability assessment is intended to be a part of an integrated mission assurance program to:

- Identify, analyze, and assess Department of Defense (DoD) assets, non-DoD assets, and infrastructure critical to projecting and sustaining DoD forces;
- Provide for asset protection and assurance; and
- Train and equip personnel to analyze, assess, protect, remediate, and restore these assets.

The DPO-MA proposal for a CIP vulnerability assessment methodology is the most recent development in a long-time process (extending from 1999 until 2003) to determine the requirements and standards for CIP vulnerability assessments. The assessment methodology would become an integral component of the CIP analysis and assessment process, which is one of six fundamental processes in the CIP program. The six CIP processes, also known as the "CIP life cycle" are analysis and assessment, remediation, indications and warning, mitigation, response, and reconstitution. The analysis and assessment process encompasses activities used to identify and analyze critical assets and their associated infrastructures, interdependencies, and single points of failure. The process covers both physical and cyber vulnerabilities of critical assets and interdependency-related single points of failure. The vulnerability assessment portion of this process determines the susceptibility of critical assets, associated infrastructures, or interdependency-related single points of failure to adverse conditions.

Vulnerability assessments differ from the other threat and risk assessment processes that exist within Defense Department risk management programs. *Threat assessment*—the process of identifying and evaluating threats to critical assets, infrastructures, or single points of failure—determines the types of activities that can exploit asset vulnerabilities. *Risk assessment* combines threat and vulnerability assessments to determine the probability that an asset will be destroyed or incapacitated when a threat exploits the asset's vulnerabilities. As defined within the DoD risk management context, assessments are judgments derived from risk analysis with weighted findings using such factors as resources, operational requirements, and competing priorities to make risk acceptance decisions. DoD leaders place great importance on assessment methodologies that help them most completely understand all risks to assets.

While vulnerability assessment methodologies in general predate the Defense Department's CIP program, the Department has not designated any current methodology or combination of methodologies as a DoD-wide standard for its CIP program. This situation, however, is changing. As stated in the first paragraph, the Defense Department is moving ahead to develop a standard process that will capitalize on four years of experience gained from applying combinations of existing vulnerability assessment methods to specific CIP requirements.

The Purpose of This Report. This report was prepared to support the CIP Director's strategy for Outreach, Education, and Training. It seeks to help those interested in understanding the Defense Department's current concepts and plans for developing CIP-specific vulnerability assessments. It describes the department's experiences in conducting vulnerability assessments and in searching for the specific characteristics and processes most appropriate for a CIP program methodology. The report ties together and summarizes the many documents that were prepared from 1998 until 2003 and that cover assessment descriptions, applications, information sharing, and a range of other issues related to assessment methodology. Annex B provides a summary of the problems found and the solutions recommended in each of DoD's CIP vulnerability assessment studies conducted from 1999 until 2003.

This report addresses each of the following questions in its own section:

1. How is vulnerability assessment defined within a national defense context?
2. How do vulnerability assessments contribute to the DoD CIP program?
3. What are the characteristics of vulnerability assessment methodologies commonly used for the CIP program?
4. Is there a common basis for standardizing the CIP vulnerability assessment process?
5. What is the current plan for developing a standard CIP vulnerability assessment methodology?

Numerous footnotes provide references to additional details for those seeking more information about the subject. These footnotes plus the annotated bibliography in Annex B provides a comprehensive reference base for gaining background knowledge about vulnerability assessments in general and about the DoD CIP program in particular. This report and all the bolded references in Annex C can be found online at the DoD CIP portal at http://www.dod-map.msiac.dmso.mil.

SECTION 1 - DEFINING VULNERABILITY ASSESSMENT WITHIN A NATIONAL DEFENSE CONTEXT

What Is Vulnerability Assessment?

The concept of vulnerability assessment was well established in risk management literature before its use in U.S. national and DoD CIP programs. Risk management is defined as a systematic analytical process that considers the likelihood that a threat will disrupt an asset and that identifies actions to reduce the risk and mitigate the consequences of the disruption.[1] Risk management principles generally acknowledge that while not all risks can be eliminated, determining sources of threats, their effects, and ways to mitigate them can reduce most risks.

The Simple Risk Model shown in Figure 1.1 illustrates the risk management process. Originally developed by the previous OASD (C3I) CIP Directorate, the model shows the interrelationships among critical assets, threats, and vulnerability. Within these interrelationships, the category of most concern for the directorate was sector 5—critical assets that have known vulnerabilities and threat exposure. This category is where expending even limited vulnerability assessment resources will have the greatest benefit. Vulnerability assessments identify weaknesses that can be exploited by threats (e.g., hazards, hostile actions, accidents) and recommend specific actions to mitigate the vulnerabilities.

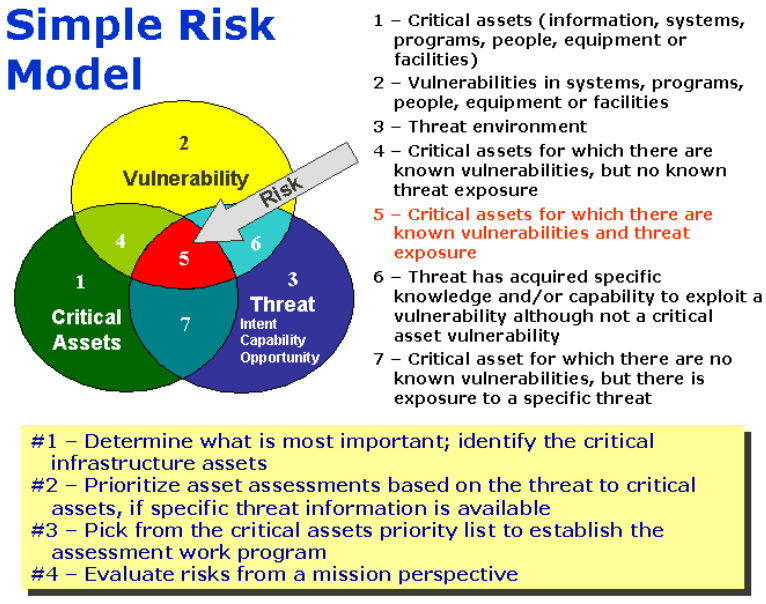

Figure 1.1 - Risk Management Model

Vulnerability assessments are used in a wide range of nongovernmental activities, including those related to insurance, financial investments, telecommunications, health, manufacturing, and security, to list only a few.

Under current DoD policy, vulnerability assessment is defined as: "The process of determining the susceptibility of critical assets, associated infrastructures, or interdependency-related single points of failure to adverse conditions." [2] This DoD definition is based on the integration of four concepts: asset susceptibility, associated infrastructures (asset dependencies), asset interdependencies, and single points of failure.

---

[1] GAO, *Homeland Security- Key Elements of a Risk Management Approach*, 12 October 2003.
[2] DoDI 3020, *Implementation of the Critical Infrastructure Protection (CIP) Program* (Draft), March 2003.

Asset susceptibility means than an asset is vulnerable to one or more threats. As shown in Figure 1.1, activities become threats to an asset when there is intent, capability, and opportunity to harm an asset. Assets are susceptible when their characteristics make them vulnerable to one or more threats. Within the CIP context, vulnerability is defined as: "The characteristics of a system which cause it to suffer a definite degradation (inability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment."[3] As a concept, therefore, susceptibility and vulnerability are linked terms when a threat is present and able to exploit vulnerability, which can make the asset susceptible to system failure.

Take, for example, control systems, which include supervisory control and data acquisition (SCADA) systems. These computer-based systems monitor and control sensitive automated processes and physical functions. They commonly use standardized software, are connected to other networks and often accessed from insecure remote connections, and often control multiple processes and functions. Physical threats to control units can come from damage caused by natural hazards or deliberate acts. Cyber threats can come from viruses and hacking/unauthorized access. Based on these characteristics, control systems are vulnerable to such threats as:

- Unauthorized exploitation of standardized software
- Unauthorized access from an external network
- Unauthorized access based on constraints of existing security technologies and insecure remote connections
- Damage or loss from fire, water, explosive, and blunt instrument damage[4]

Associated infrastructures are supporting assets within the same infrastructure. Other assets depend on them to function properly. Critical assets often depend on one or more associated infrastructures in order to perform their tasks properly. For example, control systems depend on other control station computers to instruct other systems to perform various functions or processes. Additionally, both a control system and subordinate control stations can depend on local cable systems to carry the electronic messages.

Asset interdependencies refer to other infrastructures and assets that permit the critical asset to perform its task. For example, a control system depends on electrical infrastructure assets to provide operating energy and on telecommunication infrastructures to communicate with switches and subordinate control stations. Each associated infrastructure has its own characteristics and threats that must be considered in the vulnerability assessment.

Single points of failure are those assets that, if lost, would stop or significantly degrade mission continuity. Single-point-of-failure assets do not have redundant assets that can perform the same task or function. With the control system, for example, the control system itself can be the single point of failure because of its unique characteristics and central function at the top of an integrated system. The vulnerability assessment process, however, seeks to find other single points of failure in the control system's associated and interdependent infrastructures, the objective being to determine system-wide vulnerabilities.

---

[3] DoDD 3020, *Critical Infrastructure Protection (CIP) Program* (Draft), 15 October 2003.
[4] GAO, *CIP – Challenges in Securing Control Systems*, 01 October 2003.

Keeping in mind how the overall DoD concept of CIP vulnerability assessment integrates this set of four concepts, in the following sections, the paper will present examples of how the vulnerability assessment concept originated, was applied, and revised to develop a standardized process to measure the vulnerabilities.

Vulnerability Assessment in National CIP Strategy

Presidential Decision Directive (PDD) 63. PDD 63 was published in May 1998 to state the Federal Government's goal to take whatever measures were necessary to eliminate any significant cyber and physical vulnerabilities from attacks on critical national infrastructures within five years (2003) from the signing of the directive. As a public-private partnership, PDD 63 assigned the Federal Government to perform essential national security missions and ensure the general public health and safety. State and local governments were charged to maintain good order and deliver minimum essential public services. The private sector was designated to ensure the orderly functioning of the economy and deliver essential telecommunication, energy, financial, and transportation services. Other points of national guidance included the development of a national infrastructure assurance plan, the allocation of 19 specific infrastructure sector responsibilities to various Federal agencies, and the identification of sector performance tasks.

PDD 63 stated the following requirement for vulnerability analysis as a specific national task:

"*For each sector of the economy and each sector of the government that might be the target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector*."[5]

This task was to be accomplished in conjunction with related tasks to remediate detected vulnerabilities, to collect and analyze foreign threats and warn about pending attacks or hazards, to plan for response and reconstitution following attacks or hazard incidents, and to require Federal actions to accomplish international, legislative, and budgetary tasks. Additionally, PDD 63 required Federal agencies to develop implementation plans within 180 days following the directive's announcement. DoD's response was to develop and publish the DoD CIP Plan (addressed later in this section) in November 1998.

Current Federal Strategy for Homeland Security. The intent of the Bush Administration's *National Strategy for Homeland Security* is to build Federal, non-Federal, and private sector cooperation for homeland security. The National Strategy identifies short-term and long-term Administration, Federal, non-Federal, and private sector goals to secure the U.S. homeland from terrorist attacks. It identifies six critical mission areas, as shown in Figure 1.2. The National Strategy addresses vulnerability assessments within two of the six critical mission areas: intelligence and warning, and protecting critical infrastructures and key assets.[6]

While not specifically defined in the National Strategy, vulnerability assessments are described as an integral part of the intelligence cycle within the intelligence and warning mission area. Listed as one of four distinct categories of intelligence and information

---

[5] The White House, Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection,* May 1998.
[6] Office of Homeland Security, *National Strategy for Homeland Security*, July 2002.

analysis, vulnerability assessment is described as allowing planners to "… project the consequences of possible terrorist attacks against specific facilities or different sectors of the economy or government." These projections would allow Federal and non-Federal authorities to strengthen defenses against different threats.

Assessments can be facilitated by using tools like computer modeling and analysis as part of a careful analytical process to ensure that the correct infrastructure assets are protected. The National Strategy's vulnerability assessment category links the Strategic Analysis of the Enemy and the Tactical Threat Analysis categories with the Threat-Vulnerability Integration category. This sequence permits mapping terrorist threats and capabilities, both current and future, against specific facility and sector vulnerabilities. This further permits authorities to determine which organizations pose the greatest threats and which sectors, facilities, and assets are most at risk. It can also allow planners to develop thresholds for preemptive or protective action.

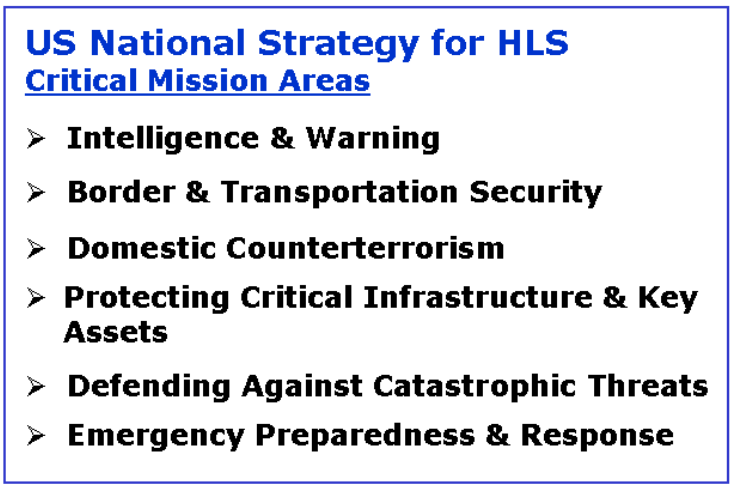

Figure 1.2 – Mission Areas: US National Strategy for HLS

To provide a complete, current, and accurate assessment database, the Department of Homeland Security will eventually collect and store vulnerability assessments of critical targets across critical infrastructure sectors when acting as a "Protecting Critical Infrastructures and Key Asset" component of the National Strategy. According to statements in the National Strategy, this capability will give the department the ability to translate threat information into prevention and mitigation action in the shortest time possible. The National Strategy plan views the abilities to continuously evaluate threat information against U.S. vulnerabilities, inform the President, issue warnings, and effect action as crucial.

The National Strategy also identifies as crucial the need for sharing vulnerability assessment information between Federal and non-Federal agencies, and particularly with the private sector. To do this effectively, the "law" section of the National Strategy recommends that an Attorney General-led panel propose the legal changes needed to enable the sharing of essential security information. The legal changes would give the private sector reasonable assurance that good faith disclosures about vulnerabilities and preparedness would not expose firms to liability, a drop on share value, loss of competitive advantage, or antitrust action.

Vulnerability Assessment in Early Defense Department CIP Planning

The start of the current DoD-wide concept of CIP vulnerability assessments began with establishing a separate DoD CIP Directorate and releasing official guidance and policy for implementing a CIP assessment process.

1998 Department of Defense Critical Infrastructure Protection Plan. Published in November 1998 in response to PDD 63 requirements, the DoD CIP Plan was developed as a guide for the department's component organizations to ensure that the infrastructure assets that DoD uses to execute its missions and functions are available when needed. The CIP Plan first identified the DoD elements (e.g., facilities, equipment, information systems, people, and contracts) used to meet defense missions, which helped determine what assets are critical. The plan also explained how to identify an asset's associated vulnerabilities, its interdependencies, and the measures needed to protect them.

The original CIP program leveraged current DoD capabilities and integrated CIP with related programs. Examples of related programs include the Defense Information Assurance Program (DIAP), the Critical Asset Assurance Program (CAAP), and the Infrastructure Assurance Protection (IAP) Program. The DoD CIP Plan sought to achieve critical infrastructure assurance through applying six business practices. These practices, known as the CIP life cycle, include analysis and assessment, remediation, indications and warning, mitigation, response, and reconstitution. Figure 1.3 illustrates the relationships among the CIP life cycle events. The CIP Plan explained how these practices would be coordinated and reconciled among the CIP component organizations, such as the DoD asset owners, DoD installations, DoD infrastructure sector lead agencies, Military Services, DoD special function lead agencies, and the Joint Staff.

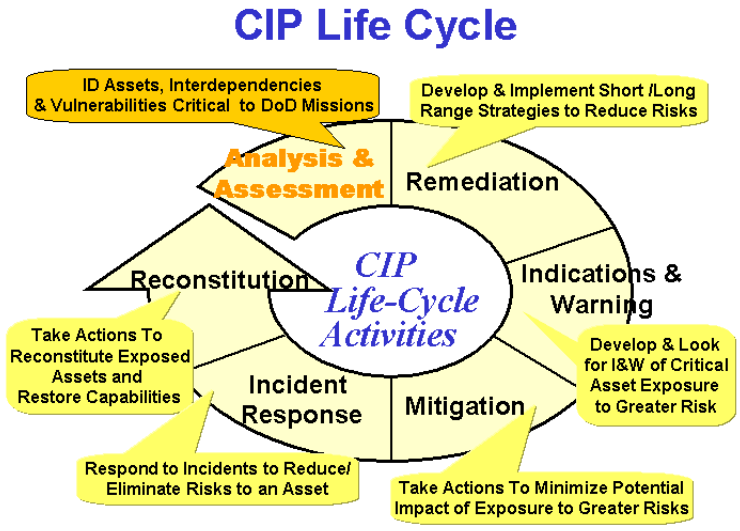

Figure 1.3 – DoD CIP Life Cycle of Events

The CIP Plan directed that the DoD CIP vulnerability process be conducted as a part of CAAP. This meant that all critical assets would have an associated baseline vulnerability index calculated from the inputs associated with a class of asset and its geographic region. The vulnerability index included the probability of natural disasters, criminal or national security threats, technological failures, and similar categories. Information about operational readiness and emergency preparedness was to be associated

with the critical asset and factored into the vulnerability rating. Operational readiness and emergency preparedness information was to be provided from several levels:[7]

- DoD critical asset owners would provide asset-level vulnerability assessment data
- DoD installations would provide installation-level vulnerability assessment data
- Defense infrastructure sector lead agencies would provide sector-level vulnerability assessment data
- The Defense Functional Coordinator for CIP would provide DoD-wide vulnerability assessment data
- National sector liaison officials would provide national sector vulnerability assessment data
- The National Infrastructure Protection Center (NIPC) would provide nationwide vulnerability assessment data

Absent from this contributor list are the Combatant Commanders, who would provide vulnerability assessment data for theater missions. Also not mentioned is the requirement to combine all this data into a comprehensive, integrated view of the asset's vulnerabilities in regard to other dependent or interdependent infrastructure assets, both DoD and non-DoD. Without integration, the data from these multiple collection processes could lead toward "stovepiping," meaning that information is narrowly shared between agencies.

DoD Directive (DoDD) 5160.54 (CAAP). This directive established CAAP in January 1998 to implement the requirements in Executive Order 12656, Assignment of Emergency Preparedness Responsibilities. In the absence of formal approval of new CIP policy in DoDD 3020 and DoD Instruction 3020, CAAP remains current CIP policy.

CAAP is a set of processes, tools, and information intended to assist DoD's critical asset owners, installation commanders, components, sector lead agencies, and special function coordinators. Its aim is to improve DoD's mission readiness by accounting for dependencies on assets and infrastructures using the joint deliberate and crisis action planning process. The policy directed the establishment of an "…integrated infrastructure vulnerability assessment program based on an analysis of the identified Critical Assets using risk management principles that will provide the information necessary to effectively allocate available resources necessary for assurance."[8]

The DoD CIP Plan interpreted the vulnerability assessment emphasis in CAAP as a process to improve asset assurance. This would be accomplished by standardizing the ways to determine DoD and non-DoD asset criticality and by developing vulnerability metrics, thus enabling the remediation process to be based on established and reliable criticality and vulnerability standards. The plan refers to "criticality attributes," which are elements of information required to determine an asset's criticality. Some of this information is baseline or static data that is independent of time or situation and can be routinely identified and collected. Other asset information can be dynamic and depend on time and situational factors. Over time, as user requirements and asset information mature, criticality attributes may be aggregated into a "criticality index" such as a numeric scale. The index could be used

[7] DASD (S&IO), *Department of Defense Critical Infrastructure Protection (CIP) Plan*, November 1998.
[8] DoD Directive 5160.54, *Critical Asset Assurance Program (CAAP),* January 1998.

for asset comparison, data display, and data reference. Similarly, "vulnerability attributes" can be developed for baseline information and for situational information about asset vulnerability. Collected following an analysis of asset vulnerability assessment data, the information would be aggregated into a "vulnerability index." The outcome would be a "vulnerability ratio," which could compare criticality and vulnerability indices, which in turn can be used as a remediation decision tool to allocate resources.

The described process requires stakeholder (e.g., installation commanders, asset owners, assessment agencies) agreement on a comprehensive standard process for CIP vulnerability assessments. Unfortunately, there is no current agreed-upon standard, and CIP components currently use several assessment processes. The lack of agreement remains despite four years of experience conducting vulnerability assessment demonstration projects designed to evaluate the elements needed for a CIP vulnerability assessment standard, and despite two major CIP Directorate-sponsored vulnerability assessment studies recommending standardization. The change of CIP management from ASD (C3I) to ASD (HD) has renewed interest in achieving a standard CIP process. Sections 3 through Five of this report describe current CIP-related vulnerability assessments, the outcomes of the vulnerability assessment studies, and the scope for the planned development of a standardized CIP assessment.

A Sample DoD Vulnerability Assessment Application. As a DoD process, vulnerability assessments existed before the release of the CIP Plan and DoDD 5160.54. A critical element of risk management practices, vulnerability assessment was a highly developed element of DoD's security risk management programs. One DoD program, the Antiterrorism/Force Protection (AT/FP) program, makes extensive use of the vulnerability assessment process. This program is different but complementary to the DoD CIP program. The DoD CIP program is concerned about assuring the viability of infrastructure assets critical to DoD-wide mission success, while the AT/FP program focuses primarily on protecting installations and the personnel, facilities, and equipment assigned to or physically located on the installation. However, asset information gained from the AT/AP program is an important source of criticality and vulnerability information for the CIP program.

The AT/FP program defines vulnerability assessments with a fixed site emphasis as:

"*An evaluation (assessment) to determine the vulnerability to a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. The process the commander uses to determine the susceptibility to attacks from the full range of threats to the security of personnel, family members, and facilities, which provide a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks*." [9]

To assess vulnerabilities to DoD installations, the AT/FP program uses the Joint Staff Integrated Vulnerability Assessment (JSIVA) methodology. JSIVA reviews physical security measures, AT/FP training, operational intelligence fusion, structures, and plans for responding to terrorist incidents.

Developed and conducted by the Defense Threat Reduction Agency (DTRA), the JSIVA methodology is only one of several DTRA responsibilities in support of the DoD AT/FP program. DTRA is also tasked to support Combatant Commands, Military Services, and the Joint Staff with vulnerability assessments of exercises, airports and seaports of

[9] ASD (SO/LIC), DoDD 2000.12, *DoD Antiterrorism (AT) Program*, 13 April 1999.

embarkation/debarkation, and in-transit forces. Copies of all DTRA-conducted assessments are provided to the DoD Counterintelligence Field Activity (CIFA) for analysis of terrorist threats against U.S. targets. DTRA maintains a vulnerability assessment database interoperable with the Defense Intelligence Agency and the Joint Intelligence Task Force for Counterterrorism. DTRA also provides periodic analyses to the Chairman of the Joint Chiefs of Staff. These analyses can supply useful information for CIP program activities supporting Combatant Command and Military Service operational mission assurance. Finally, the AT/FP program tasks DTRA to provide follow-up assistance (e.g., training organizational staff about remedial actions or using self-assessments to sustain AT/FP readiness) to assessed organizations.

DTRA's JSIVA process on behalf of the DoD AT/FP program clearly provides complementary support to the CIP vulnerability assessment process. With its emphasis on installation and fixed-site infrastructure assessments, JSIVA can provide useful information about asset criticality and vulnerability. Two components—the JSIVA database and the assessment reports to CIFA—can provide asset characterization, vulnerability, and remedial action information that can be important input to the CIP program's analysis and assessment process. Subsequent sections of this report address the relationships between the characteristics of DTRA's vulnerability assessment programs and the requirements for a CIP vulnerability assessment in more detail.

SECTION 2 - THE CIP FUNCTION OF VULNERABILITY ASSESSMENTS

Section 1 introduced the concept of a vulnerability assessment process that serves the security interests of the United States and the Defense Department. This section explains how the vulnerability assessment process contributes to the DoD CIP program. It focuses on the important role the vulnerability assessment process has within the CIP Directorate's DoD CIP Strategy and within the Nine-Step Analysis and Assessment process of the Joint Program Office for Special Technology Countermeasures (JPO-STC). This explanation is necessary to understanding the range of vulnerability assessment methodologies currently supporting the DoD CIP program.

CIP Is About Mission Assurance

Bill Bryan, CIP Director, OASD (HD), connected the term "mission assurance" to the CIP program when he took it over in 2003. In presentations to the many DoD organizations that make up the CIP constituents, Bryan emphasized that the CIP program is more than the protection of critical assets and that it encompasses more than the physical security of DoD infrastructures and assets. The CIP program addresses the interdependencies among critical DoD and non-DoD infrastructure assets and Defense Industrial Base capabilities, both foreign and domestic and both public and private. CIP is global, enveloping homeland support facilities and assets in forward theaters of operations abroad. CIP Director Bryan emphasizes that the CIP program is an integrating activity for mission assurance, including determinations of what is critical, what is vulnerable, and what must be done to lower risk. Once these determinations are made, protecting an asset may become one of several options for remediation or mitigation.[10]

"Mission assurance" entered the CIP context during the U.S. Pacific Command's (USPACOM) Appendix 16 Pilot Analysis and Assessment Project. However, it has not yet been formally defined in CIP program policies and documents. OASD (C3I) CIP Directorate and the Joint Staff jointly sponsored the Appendix 16 project. The Joint Staff designated USPACOM as the "lead Combatant Command" to develop a standard repeatable mission analysis and assessment process, and USPACOM conducted the Appendix 16 project in collaboration with JPO-STC from February 2002 until April 2003.[11]

Appendix 16 developed the concept of Mission Essential Requirements (MERs), which are the elements needed to accomplish a defined operational mission. MERs are linked to specific forces, functions, tasks, services, and infrastructure assets. The output from this identification process is called Mission Area Analysis (MAA). As shown in Figure 2.1, outputs from the MAA process become the inputs to the Appendix 16 assessment process. The assessment identifies critical asset vulnerabilities, recommends remediation options, analyzes the impact on a mission of losing an asset, and reviews operational continuity plans

[10] William Bryan (Director CIP/OASD (HD)), briefing to the Intelligence Surveillance and Reconnaissance Conference, 19 August 2003.
[11] USPACOM, OPORD 3020 *Critical Infrastructure Protection* (Draft) (Unclassified/FOUO), January 2003.

in event of losing an asset. The process gives a command-wide visibility to mission essential assets, their vulnerabilities, and most importantly, identifies actions that should be taken to mitigate any potential loss of a mission-supporting asset. The Appendix 16 CIP analysis and assessment process provides Combatant Commanders with a measure of "mission assurance" by letting them see how disruptions or loss of critical infrastructure assets will be mitigated to permit the execution of their missions.

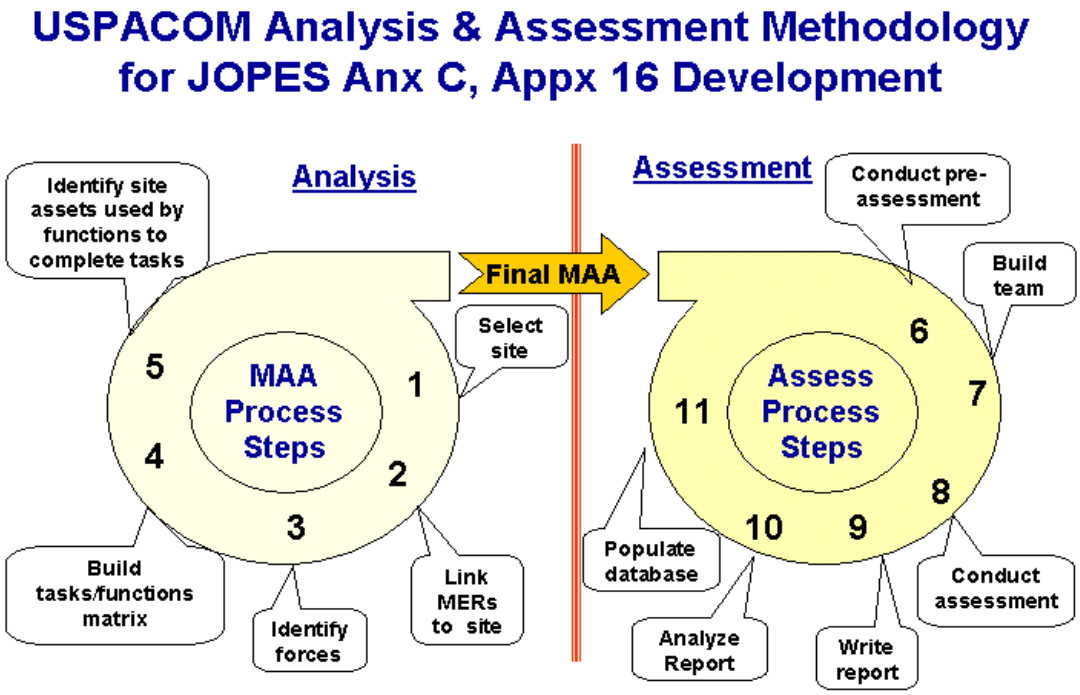

Figure 2.1 – USPACOM Analysis and Assessment Methodology

CIP Strategy for Analysis and Assessment

As the foregoing example illustrates, vulnerability assessment is a fundamental component of the Defense Department's CIP program. It is a linking element in the CIP risk management process, connecting the identification of critical assets for mission assurance with the measures and actions taken to either protect them or mitigate their loss or disruption.

DoD CIP Strategy. In the published CIP Strategy, vulnerability assessment is a significant component in the analysis and assessment life cycle area. The purpose of analysis and assessment is to:

- "Determine what assets are truly critical mission independent and those tied to specific missions, including identification of support infrastructure assets, their dependency on other assets
- Identify vulnerabilities that could result in degradation or disruption of missions, regardless of the cause

- Determine the consequences of cascading failures on operations, and identify possible corrective actions"[12]

The products of the analysis and assessment process include:

- "A characterized enumeration of DoD critical infrastructure assets
- Comprehensive, tailored CIP vulnerability assessments on selected critical infrastructure assets
- Risk-based recommendations for remediation of vulnerabilities presented to Combatant Commanders, asset owners, and DoD policy officials, and submitted into the national infrastructure protection process."[13]

The DoD CIP Strategy for identifying critical assets consists of two converging efforts that identify (1) scenario-independent (or non-scenario-dependent) and (2) scenario-dependent critical infrastructure assets. Disruption of scenario-independent critical infrastructure assets would adversely influence multiple missions, or day-to-day operations, and perhaps national decision making regarding national or economic security. Knowing the interdependencies of these assets and the consequences of their degradation provides essential input to risk management decisions and to the allocation of resources for remediation and mitigation. Disruption of scenario-dependent critical infrastructure assets would adversely influence a particular mission. Knowing the interdependencies of these assets and the consequences of their degradation provides essential input to risk management decisions for specific operational missions.

The DoD CIP Strategy states that a fundamental part of the CIP program requires conducting comprehensive, tailored CIP vulnerability assessments on both scenario-independent and scenario-dependent critical infrastructure assets only after identifying, validating, and prioritizing vulnerability assessment requirements. In this way, DoD can preserve scarce vulnerability assessment resources and skills for the most important assets. The goal of CIP vulnerability assessments is to achieve greater fidelity of information available to the senior DoD leadership and Combatant Commanders for assessing risks to critical assets and, consequently, to military capabilities and operations. Additionally, CIP vulnerability assessments should enable infrastructure asset owners to support vulnerability remediation and mitigation plans, decisions, and resource allocation. These assessments will also support the implementation of mitigation activities to reduce or minimize the operational impact of exploited vulnerabilities. An equally important output of the assessment process is the information generated for developing operational risk management protocols.

Nearly every DoD department or agency engages in some form of vulnerability assessment. Several DoD agencies have units that specialize in internal vulnerability assessments and/or vulnerability assessments at the request of external organizations.[14] To facilitate a more cohesive approach for allocating resources for assessments, the DoD CIP Strategy for vulnerability assessments seeks to employ three basic approaches:

---

[12] OASD (C3I) CIP Directorate, *Department of Defense Critical Infrastructure Protection Strategy* (Unclassified/FOUO), April 2003.
[13] Op. cit.
[14] OASD (C3I) CIP Directorate/Joint Staff J-5, *Integrated Vulnerability Assessment – Integrated Process Team Final Report*, July 2001.

- CIP vulnerability assessments conducted on scenario-independent critical infrastructure assets by experts who are independent of the asset owner
- Vulnerability self-assessments conducted by asset owners at the DoD component or sub-component level
- CIP analysis and assessment for National Special Security Events (NSSE) in support
  of Military Assistance to Civil Authorities (MACA) missions

These approaches achieve a design for a comprehensive and tailored assessment process, which can preserve scarce resources. By focusing assessments on scenario-independent critical infrastructure assets, the CIP Strategy concentrates limited assessment resources on those assets having the greatest interdependencies within multiple DoD missions and functions. Second, by emphasizing DoD component self-assessments, asset vulnerabilities (those most easily assessed and mitigated using organic capabilities) can be addressed without using scarce external assessment specialists. Finally, an assessment focus on NSSE support to civil authorities requires DoD to develop assessment processes and protocols with possible unique capabilities to assess a range of non-DoD assets. Developing these capabilities can assist DoD's ability to better assess infrastructure asset vulnerabilities within the Defense Industrial Base community and for foreign assets supporting overseas DoD missions.

CIP Program Office Responsibilities. As of October 2003, the new CIP program management office, the Defense Program Office for Mission Assurance (DPO-MA), is responsible for synchronizing the multiple vulnerability assessment programs into an integrated and standardized CIP assessment process. DPO-MA assumed this responsibility from JPO-STC, which had been originally tasked by DoD Directive 5160.54 to provide infrastructure assurance analysis and vulnerability assessment support to the DoD executive agent for CIP:

"*The Secretary of the Navy shall require the Program Manager, Joint Program Office for Special Technology Countermeasures, to provide the infrastructure assurance analysis and vulnerability assessment support to the DoD Executive Agent*."

Thus, JPO-STC became responsible for providing technical assistance to DoD CIP component organizations for the entire range of analysis and assessment activities. From 1999 until 2003, this technical assistance included analysis tool development, asset database development, vulnerability assessment development for both scenario-independent and scenario-dependent assets, and internal staffing assistance.

Under its new functional responsibilities, DPO-MA will implement the DoD CIP Strategy for vulnerability assessments by:

- "Establishing, coordinating and maintaining a critical infrastructure vulnerability and special technology vulnerability assessment process, including protocols, procedures, reporting criteria, data repository and information sharing guidelines
- Coordinating CIP-related site surveys and vulnerability assessments with the Joint Staff, Combatant Commands, the Military Services, and DoD agencies

- Assisting the DoD CIP Director in oversight and approval of CIP assessment scheduling and prioritization, through coordination and leadership of scheduling conferences." [15]

DoD CIP Application of Vulnerability Assessments

Background. The CIP vulnerability assessment process is not a standalone activity. It is an integral part of the CIP analysis and assessment process. However, no CIP vulnerability assessment methodology exists that applies to all components repeatedly and consistently based on recognized standards. Findings in the OSD *Integrated Vulnerability Assessment Integrated Process Team Final Report* (2001) reveal that the CIP components use 22 different assessment products. All of these assessment products were developed for specific organizational requirements, while some, such as JPO-STC's Infrastructure Assurance Program Vulnerability Assessment, was revised for wider CIP purposes. In this case, the IAP assessment was adjusted to support analysis and assessment methodologies for the USPACOM Appendix 16 Pilot Project.

One possible reason for the previous lack of effort in developing a standardized CIP assessment process was the absence of an approved policy to govern the DoD CIP program and to provide an authorized basis to develop specific CIP standards for performance. Previous guidance from DoDD 5160.54 did not provide enough details for program development, and the DoD CIP Plan was a concept plan, not a fully approved and vetted authorization document. The OASD (C3I) CIP Directorate sought to achieve specific program policy through the development, coordination, and approval of DoDD 3020, *Critical Infrastructure Protection (CIP) Program*, and DoDI 3020, *Instructions for the Critical Infrastructure Protection (CIP) Program*. Unfortunately, both documents experienced prolonged difficulties in finding concurrence, and then their approval was delayed during the DoD staff reorganization.

As the CIP policy coordination and approval process was under way, concurrent and decentralized procedural developments were being made by the Military Services and DoD agencies to develop tailored CIP assessment methodologies.[16] The Army and Air Force developments were closely tied to their AT/FP programs. The Navy and Marine Corps developments sought to integrate existing physical, personnel, and information security assessments with JPO-STC's supporting commercial infrastructure assessments. This later approach was reported by some of the DoD infrastructure sector lead agencies, such as Finance, Logistics, Transportation, Global Information Grid (GIG/C2), Space, and Intelligence Surveillance and Reconnaissance (ISR).

Nine-Step Analysis and Assessment Methodology. Another activity that gave the CIP vulnerability assessment process a framework for development was JPO-STC's development of the Nine-Step Analysis and Assessment methodology. In late 2002, JPO-STC proposed a standard analysis and assessment methodology that could apply to all CIP components.[17] JPO-STC conceived the methodology before its involvement in USPACOM's Appendix 16 project. During its involvement, JPO-STC revised and tested its methodology, later applying

---

[15] OASD (HD) CIP Director, *Functional Responsibilities Document* (Draft), September 2003.
[16] OASD (C3I) CIP Directorate, *DoD FY 2002 CIP Annual Report*, 30 April 2003.
[17] JPO-STC, *A Standard DoD Critical Infrastructure Protection Analysis and Assessment Process*, November 2002.

it to support the sector lead agencies in developing their Defense Infrastructure Sector Assurance Plans (DISAP). The current nine-step methodology is the result of this two-year collaboration. Many of the sector lead agencies and Combatant Command CIP planning staffs use it in their CIP risk management activities. The proposed standard methodology consists of nine steps that focus on DoD missions and specifically answer the following questions:

- What are the critical assets for conducting and supporting the mission or sector?
- If an asset is determined to be critical, is it vulnerable and to what?
- What can be done to assure the availability of the asset?

Figure 2.2 shows each of the nine steps. The first part of the process identifies assets that are critical to executing the mission. They are referred to as critical Mission Required Assets (MRAs) and Infrastructure Supporting Assets (ISA).

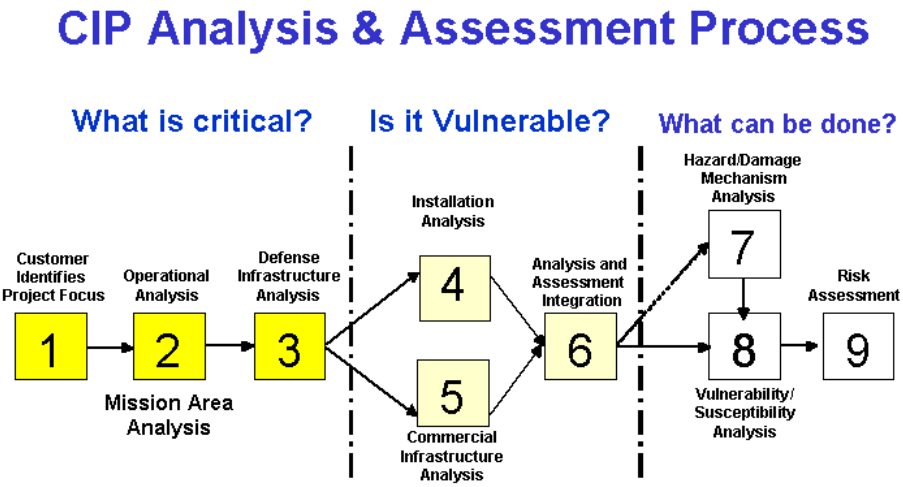

Figure 2.2 – JPO-STC Nine-Step Analysis and Assessment Process

Step One. Defense organizations determine which mission tasks must be analyzed and which must have assured infrastructure-supporting assets.

Step Two. The mission is analyzed to identify MRAs, which are the major tasks that must be accomplished for mission success.

Step Three. Analysts identify specific supporting ISAs and systems for each critical task supporting an MRA. Using the organization's mission parameters, the analysts determine asset priorities based on asset criticality. This priority and location list establishes the priority for the vulnerability assessment portion of the process.

Using the findings from the first three steps, the next section of the methodology conducts the vulnerability assessment and analyzes the results.

Step Four. DoD organizations select critical installation sites for assessment based on recommended lists developed in step three. The assessment organization coordinates with onsite officials before the site visit. The onsite assessment identifies asset capabilities, vulnerabilities, and dependencies on other onsite systems and assets; the assessment then develops recommendations to mitigate and remediate vulnerabilities.

Step Five. Commercial infrastructures follow an assessment process similar to step four, although a commercial onsite visit takes place only if required and permitted by the

commercial asset or infrastructure owner. Instead, the assessment organization extensively researches data and develops information about the commercial asset to determine capabilities, vulnerabilities, dependencies, and a range of remediation recommendations.

Step Six. The information gathered in steps four and five is integrated, with emphasis on verifying the completeness of the assessment information and connectivity between DoD installations and commercial assets.

Developing risk assessment remediation requirements is the objective in the third component of this methodology.

Step Seven. This step is an ongoing process that can be conducted in parallel with the rest of the analysis and assessment process. This step reviews all the possible natural and manmade hazards, damage mechanisms, and technical limitations that can disrupt assets.

Step Eight. The hazard and damage analysis is integrated into the vulnerability analysis for all MRAs identified in steps four through six. The analysis identifies required remediation actions for each critical asset and hazard combination.

Step Nine. The analysis team collaboratively develops a recommended risk-based assessment plan for all the critical and vulnerable assets specific to the mission. This recommendation is aimed at assisting organizational decision makers to implement the most efficient enhancements for critical asset assurance.

While the methodology does not specify a particular vulnerability assessment product or process, the vulnerability assessment method used requires certain consistent inputs and outputs. The required inputs and outputs are shown in Table 2.1. Consistency in both the categories of data inputs to the selected assessment method and the categories of data outputs are important to enabling the JPO-STC analysis and assessment methodology to recommend remediation options.

Vulnerability Assessment Is a Vital CIP Function

The DoD CIP Strategy established a vital function for vulnerability assessment as a component of the analysis and assessment activity. In both the USPACOM Appendix 16 development and in the proposed JPO-STC Nine-Step Analysis and Assessment methodology, vulnerability assessments are essential in identifying infrastructure asset vulnerabilities and generating remediation options. They provide the basis for mission impact analysis due to loss of the asset and generate continuity of operations plans for command in the event of asset loss. Important in the decision to use vulnerability assessment resources is the identification and characterization of the most mission critical infrastructure assets, both DoD and non-DoD. The "analysis" component of the analysis and assessment process establishes guidelines for critical asset identification and characterization, with CIP Strategy priority to scenario independent critical assets.

The OASD (C3I) CIP Directorate's DoD CIP Strategy document did not specify specific appropriate methodologies or assessment agencies appropriate for CIP-specific assessments. Instead, the strategy stated three approaches where available assessments could be applied in a tailored and focused manner to address specific assessment requirements and preserve scarce assessment resources. However, in the OASD (HD) CIP Director guidance to the new CIP program office, there is a stated emphasis in establishing and controlling a centralized

vulnerability assessment process. In response, in October 2003 the DPO-MA released its initial proposal for a standardized process, which will be discussed in Section 5 of this report. Before doing so, it is worthwhile to review current assessment methodologies and the CIP program experience in developing a standardized process. This review can be found in Sections 3 and 4 of this report.

Required Inputs

- Mission component priorities
- Asset mission criticality
- Prioritized mission essential requirements (MER)
- Critical mission required assets (MRA) linked to MERs
- Identified mission tasks employing specific MRAs
- Identified MRA intra- and inter-dependencies
- Prioritized list of critical DoD MRA locations and specific sites for assessment
- Prioritized list of critical non-DoD MRA locations and specific sites for assessment

Required Outputs

- MRA susceptibility and vulnerability information
- Verification or revision of on-site MRA critical priorities
- Verification or revision of MRA "Dependency Paths" to other MRAs
- Verified information and data on critical commercial infrastructure asset vulnerabilities and "Dependency Paths"
- Natural hazard and damage information
- Integrated DoD and non-DoD MRA susceptibilities, vulnerabilities, and dependency paths
- Remediation recommendations

Table 2.1 Required Vulnerability Assessment Instrument Inputs and Outputs to Support the JPO-STC Proposed Standard CIP Analysis and Assessment Process

SECTION 3 – CHARACTERISTICS OF VULNERABILITY ASSESSMENTS COMMONLY USED FOR THE CIP PROGRAM

So far, the information in this report has shown how vulnerability assessment is a critical functional component of the CIP analysis and assessment process. The concepts used to implement a DoD CIP vulnerability assessment process are rooted in risk management practice, which predated the DoD CIP program and firmly established the concept and application of vulnerability assessments. Additionally, guidance in DoDD 5160.54 (1998), the DoD CIP Plan (1998), and the DoD CIP Strategy (2003) described the central role of vulnerability assessments in the CIP program's effort to assemble resources and prepare plans to mitigate identified vulnerabilities. Finally, the general functions of vulnerability assessments were described in examples from the AT/FP program, the operation of the Appendix 16 methodology, and JPO-STC's Nine-Step Analysis and Assessment process.

Section 3 focuses on delineating the characteristics of the vulnerability assessment methodologies commonly used in the DoD CIP program. It identifies and describes the most frequently used assessment methods within the CIP component community. The primary sources for the descriptions are the Integrated Vulnerability Assessment/Integrated Process Team *Matrix of Vulnerability Assessments* (2001), the Integrated Vulnerability Assessment Requirements Team survey (2003), and the JPO-STC *Vulnerability Assessment Catalog* (2003). Detailing all the different protocols, standards, and procedures used in each assessment would repeat the details already provided in these references, so this section simply summarizes the key distinctive features of several of the most commonly used methods.

Many DoD Critical Assets and Many Vulnerability Assessments

Following the requirements established by PDD 63 and DoDD 5160.54 in 1998, the CIP component agencies have identified hundreds of critical assets within numerous databases. As discussed in Section 2, critical assets are identified during the analysis phase of the analysis and assessment process. Once the assets are identified and their mission tasks, functions, and physical attributes characterized, they are entered into a classified database. Presently, DoD critical assets are listed in a variety of separate databases maintained by the DoD Infrastructure Sector Lead agencies, the Combatant Commands, the Military Departments, JPO-STC, and the Joint Staff.

The Joint Staff's Mission Assurance Asset Database (MAAD) is a representative example of a CIP-related asset database. It contains about 1,400 mission-critical assets identified by the Combatant Commands, Military departments, and DoD agencies. The Joint Staff directed JPO-STC to establish MAAD following the terrorist attacks of September 11. Assets included in the database were selected based on user-defined weight factors.[18] The initial input of assets included buildings, military units, DoD research laboratories, power plants, depots, substations, natural gas compressor plants, wastewater treatment plants, airports, seaports, bridges, rail yards, telecommunications nodes, and numerous other examples. Later, the CIP Components added numerous other assets as an output from the JPO-STC analysis and assessment process. Other assets were added (e.g., commercial and Defense Industrial Base

[18] JPO-STC White Paper, *Mission Assurance Asset Database (MAAD)*, September 2002.

(DIB) facilities, components and technologies) following collaborative activities by the Defense Security Service (DSS) and from the Office of the Undersecretary of Defense for Acquisition, Technology & Logistics (AT&L). While MAAD is not completely suitable as an accurate repository of critical DoD assets, JPO-STC continues to upgrade it and eventually incorporate it into a CIP Integrated Data Collection and Analysis System (IDCAS). This JPO-STC proposed system would constitute an integrated and secure storage of mission-related critical assets, dependency paths, vulnerability assessment, and risk assessment information produced under the CIP analysis and assessment program.[19]

To successfully implement an IDCAS concept, the DoD CIP analysis and assessment process should lead to a standardized set of data elements. The growing acceptance of the JPO-STC Nine-Step Analysis and Assessment procedure can help the standardization process. As written, each of the nine steps would generate specific outputs. The assessment component of this process will identify vulnerabilities that could degrade or disrupt missions, determine the consequences of cascading failures on dependent and interdependent infrastructures, and finally recommend possible corrective actions. The output information and data about each assessed assets would be entered into the database by a yet-to-be-determined DoD agency. At present, however, this concept is difficult to apply because the current varieties of assessment methodologies do not lead to the similar outputs needed as standard data elements.

To understand the types of data elements generated by the various assessment methodologies, in 2001 the OASD (C3I) CIP Directorate sponsored a study. The study team, which was composed of members from most of the CIP component organizations, was to review current assessment activities for oversight control and scheduling, and also review funding, information requirements, and information sharing. The study team was also charged to make recommendations for integrating the multiple processes into a support activity to gather CIP assessment information. One of the study's findings was a matrix describing the characteristics of 22 assessment methodologies.[20]

Appendix D, Assessment Matrix, of the IVA/IPT report contained 25 data element characteristics for each of the 22 assessment methodologies. Sample data elements from the IVA/IPT assessment matrix include the following:

- Authority to conduct assessment
- Performed by
- Frequency
- Assessment standards and references
- Assessment methods
- Assets (component and DoD or public services, or industry)
- Venue (U.S. or non-U.S.)

---

[19] JPO-STC, *Critical Infrastructure Protection Database Architecture Description and Needs (Version 1.1)*, 17 March 2003.

[20] OASD (C3I) and Joint Staff J5, *Integrated Vulnerability Assessment (IVA) Integrated Process Team (IPT) Final Report*, 31 July 2001.

- Primary focus (cyber or physical)

An average of 19.6 (78.4%) of the 25 data element characteristics were completed for each of the 22 assessments. The most frequently missing characteristics were assets, venue, and primary focus. These three categories included seven sub-characteristics about the assessment's focus. The scope for the majority of the assessments was quite limited, averaging four of the seven sub-characteristics. Assessments with a wider scope (i.e., a greater number of characteristics) included the following:

- Information Assurance Vulnerability Alert (five characteristics)
- Information Assurance Readiness Review (five characteristics)
- SIPRNET Compliance Reviews (five characteristics)
- Balanced Survivability Assessments (five characteristics)
- Naval Integrated Vulnerability Assessment (six characteristics)
- NSA Information Assurance Vulnerability Assessment (six characteristics)
- NSA Operations Security (seven characteristics)
- DSS National Industrial Security Program (five characteristics)
- DSS Arms, Ammunition and Explosives Security Support (five characteristics)

Another area of interest to the IVA/IPT team's findings was the limited degree of information sharing allowed by the assessment methods. In the "Results given to" category, 20 of the 22 assessments (91%) limited report distribution to the asset owner or installation commander and the respective chain of command. The two only assessments cited that that did permit report information sharing did so only after a validated request to the assessment organization.

In other categories, the IVA/IPT matrix reflected a wide range of standards appropriate to the scope of the assessment. When individual assessments addressed different areas of asset security and vulnerability interests, any effort to integrate two or more assessments into a "CIP Assessment" will require a detailed analysis of the relationships between the standards. There was, however, a generally similar range of assessment protocols, including: pre-assessment information exchange, onsite observations and interviews, use of a pre-established checklist for recording data, periodic assessment team back-briefs to the installation or facility commanders or managers, onside exit briefing, and a final report delivered 60-120 days following the end of the assessment. Other protocols, such as defining the threat, specific remediation recommendations, tracking of remediation efforts, and follow-up activities were less uniformly conducted by the assessment teams.

One IVA/IPT study team recommendation implemented by OASD (HD) was the CIP Vulnerability Assessment Catalog. Published by OASD (HD) in September 2003, the CD-ROM listed 26 assessment types, 20 of which were previously identified in the IVA/IPT assessment matrix. The DoD CIP Directorate tasked JPO-STC to develop the catalog. However, the Directorate did not task them to develop a repository for storing assessment report results and findings because of the need to determine the proper security safeguards for the aggregated data. The release of the highly classified information from multiple sources, each requiring separate release authority, remained too complicated within the

project timeline. Instead, the catalog lists the sites assessed, assessment dates, assessment types, assessment organizations, and contact information for requesting more information.

Not yet a completed catalog of the full range and activity of the DoD assessment process, the current CD contains only 844 assessment records dating from 1997 to 2002. Of the 844 assessment records, only 8 of the 26 identified assessment types are yet represented in the catalog. The most frequently cited processes were JPO-STC's Infrastructure Assurance Program (130 records), U.S. Army Corps of Engineer's Risk Assessment Methodology - Dams (305 records), and DTRA's Joint Staff Integrated Vulnerability Assessment (JSIVA) and Balanced Survivability Assessment (BSA) (347 and 63 records respectively).[21] The table in Annex A of this report lists 19 of the catalog's most fully described assessment types and the number of their assessment reports cited on the disk.

The very number of DoD critical assets plus the many types of assessment methodologies used to determine asset vulnerabilities complicates the DoD CIP program's objective—to establish a consistent, repeatable DoD-wide vulnerability assessment process that can generate comprehensive data for analysis contributing to risk assessment decisions for remediation priorities and resources. In the near-term, the OASD (HD) CIP Director will consider recommendations from the DPO-MA about how the DoD CIP program should conduct the vulnerability assessment component of the program. One recommendation could be to develop a new, CIP program-specific assessment methodology, taking desirable elements from current assessments and combining them with new elements based on four years of experience using existing assessments to address CIP issues. Another recommendation could be to combine current assessments in an integrated and comprehensive methodology that can address scheduling, covering essential CIP data requirements, information sharing, and using reliable, consistent standards and protocols.

To better understand the considerations that DoD must make in selecting one recommendation or another, it is necessary to explain some details about the most widely used vulnerability assessment methodologies. The remainder of this section will address, in some detail, four assessment methodologies used by the CIP component community over the past 12 months. DoD extensively used three of these assessments, the JPO-STC IAP, DTRA's BSA, and JSIVA, over the past four years. They are among the most cited of the reports in the CIP Vulnerability Assessment Catalog. The fourth methodology, the Naval Integrated Vulnerability Assessment (NIVA), became operational in the past 12 months. It uses an integrative process with four different assessment types and combines them into a centralized scheduling and reporting process. It uses a process recommended in previous CIP assessment project reports and is interesting to discuss because of its similarity to the proposed DPO-MA assessment methodology.

Infrastructure Assurance Program (IAP) Vulnerability Assessment (JPO-STC)

General Information. The JPO-STC IAP vulnerability assessment is a focused approach to identifying vulnerabilities to DoD Defense Infrastructure (DI) assets and assessing non-DoD public and commercial supporting assets. The emphasis is on DI assets previously identified as

[21] JPO-STC, *DoD/JCS Vulnerability Assessment Catalog* (CD-ROM), 11 June 2003.

critical to DoD missions and functions, and tasked to support a specific Combatant Command's operational plan. Figure 3.1 summarizes the scope of this assessment.

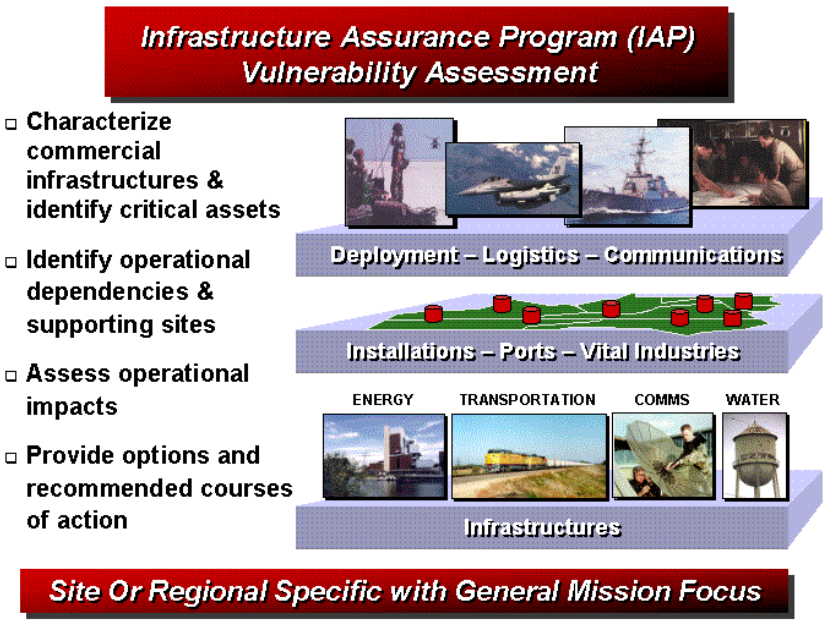

Figure 3.1 – JPO-STC Infrastructure Assurance Program

As a phase in the assessment process, JPO-STC conducts pre-assessments to identify an installation's key missions, the critical assets that support the mission/tasks, and the commercial infrastructures that support the installation's critical assets. IAP examines the installation's infrastructure assets from the perspective of their disruption or loss and the consequent impact on associated assets or operational missions.

IAP assessments are not conducted within a set site-rotation schedule, but are based on requests from organizations or facilities/installations desiring the inspection. Assessments are currently limited to U.S.-owned assets. JPO-STC is actively coordinating at Combatant Commands (e.g., USPACOM and USEUCOM) that have overseas facilities. The goal is to establish non-U.S. contacts to facilitate the assessment of foreign infrastructure assets.[22]

Assessment Teams. Two five-person to eight-person teams comprised of individuals with expertise and experience in the asset's technical and risk characteristics conduct the assessment. One team (J25) assesses assets internal to the DoD installation; others (J21 & J22) assess commercial infrastructure external to the installation. The teams often add members from other organizations to analyze specialized areas like chemical and biological sites. JPO-STC schedules approximately 15 to17 assessments annually, based on available funding and the number of assessment requests.

Standards and Methodology. The IAP standards are based on JPO-STC-developed Essential Elements of Information (EEI) checklists. These are derived from DoD policy, regulatory, and technical documents. The exact set of EEI checklists that the IAP teams use depends on the infrastructure assets to be assessed and the regional location of the site or installation. The EEI checklists give the IAP assessment teams a comprehensive list of questions for gathering data using both the EEI and their own expertise.

[22] Except where noted, the source of the information for this methodology is a written and oral interview with selected JPO-STC staff conducted by the OUSD (I) CIP Vulnerability Assessment Requirements Team, on 5 May 2003.

The IAP vulnerability assessment focuses on determining the consequences of losing a critical asset or key supporting commercial infrastructure. The nature or cause of the loss is not a central focus. The IAP assessment focuses on the mission consequences of the disruption or loss of critical assets caused by natural hazards or deliberate actions. The assessment avoids examining the nature of a specific threat or undesirable event/events that could cause the loss. Because IAP teams do not examine specific threats, assets are not assessed from the perspective of threats. Under this perspective, the IAP assessment does not analyze physical or personal security, nor does it conduct a threat analysis or assessment. Countermeasures to protect against specific types of threats are also not central to the assessment, although general observations about the lack of protective countermeasures are sometimes included in the assessment reports as secondary comments.

The IAP assessment has two concurrent steps, an installation/site mission assessment and the commercial infrastructure analysis and assessment. The installation/site mission assessment begins with the assessment sponsor selecting sites for assessment from a recommended list of critical assets located at DoD installations or sites. Before the onsite visit, the IAP team develops liaison, research, and data requirements with the sponsoring and site officials. The IAP team applies the mission-specific requirements to the assets and uses the mission and asset-specific EEI checklists to verify asset capabilities and identify vulnerabilities and susceptibilities, dependencies on other onsite infrastructure systems and assets, and potential recommendations to remediate vulnerabilities. Because of the assessment process, the IAP team develops an asset "dependency path" analysis to indicate other installations or sites and commercial infrastructure assets identified as dependencies to the assessed critical asset.

During the commercial infrastructure analysis and assessment, the IAP team conducts extensive research and data development about supporting commercial assets and infrastructures. The IAP team conducts onsite commercial asset assessments only if required by the requesting organization and with approval from the commercial asset owners or managers. Outputs from this step are verified commercial infrastructure asset information regarding asset vulnerabilities and susceptibilities, dependencies on other on-site infrastructure systems and assets, and the dependency paths to other public or commercial infrastructures and assets. For DoD assets, the IAP team recommends possible remediation for identified vulnerabilities.

Data Collection, Follow-up, and Final Report. The IAP captures initial data in a classified Excel spreadsheet to facilitate assessment data exchange and reduce the time in developing final reports. The information will later be transferred to the JPO-STC data library, which is in a Microsoft Access database available on the JPO-STC SIPRNET website. Daily information exchange takes place within the assessment team and with the installation's points of contact. However, the principal analysis of the assessment data and the development of the Final Report are conducted at JPO-STC's Dahlgren, Virginia site.

The final IAP assessment report gives detailed asset characteristics, show asset interdependency trees that show supporting infrastructures relationships to mission essential tasks, identify vulnerabilities, and estimate the potential consequences of asset disruption or loss. The report may also identify single points of failure not previously identified, plus provide observations concerning possible deficiencies in planned installation countermeasures. The IAP report may also provide a risk assessment-level rating for key assets. The IAP team subjectively assigns a rating (High, Medium, Low) to indicate a recommended prioritization for installation remediation effort. The IAP team provides reports to the installation commander and the

appropriate Combatant Commander, and retains copies on file with JPO-STC. JPO-STC will refer any requests for additional copies of the report to the sponsoring organization, which requested the assessment.

Currently, JPO-STC does not provide follow-up assessments or track the remediation of the vulnerabilities identified during their assessments. They are collaborating with PACOM to create a computer database module that Combatant Commands can use to enter their asset assessment data, which can then be used to track follow-up actions and track the status of the asset vulnerabilities and any remediation.

Balanced Survivability Assessment (BSA)

General Information. BSA is a detailed, integrated, performance-based, multidisciplinary assessment of key nodes and architectures used to execute critical missions of the U.S. and its allies. BSA assessments focus on mission continuity and revolve around measures that can improve mission assurance and survivability against a wide spectrum of threats. BSA, therefore, is not geographically oriented (e.g., toward a military base with multiple missions). Rather, BSAs provide a balanced look at a mission's survivability, providing specific prioritized recommendations to the mission's leadership to mitigate identified vulnerabilities. [23]

The stated BSA methodology is a flexible process that can be tailored to particular infrastructure assets in multiple DoD and non-DoD environments. BSA can address a wide range of assessment areas from physical, information, and personnel security to safety, emergency preparedness, nuclear, biological and chemical security; continuity of operations planning; support to infrastructure networks; and threat/hazard analysis.[24] BSA teams use an assessment methodology in which each specialty area is guided by a set of approved protocols or guidelines. Each BSA team specialist must be completely familiar with the applicable DoD and civilian technical codes and standards. DTRA selects and trains team members to enhance their expertise and their ability to apply good judgment and best practices.

These capabilities have given the DTRA BSA a broad applicability to both DoD and non-DoD facilities and installations. These sites have included strategic underground command centers, the Pentagon, communication and satellite control nodes, intelligence community sites, Combatant Command headquarters, critical U.S. ports, U.S. Olympic law enforcement command centers, and numerous others for the Departments of Interior, Transportation, and Justice. In addition, by building on a nodal approach, DTRA has conducted BSA analyses of entire mission architectures such as the former U.S. Space Command's Integrated Tactical Warning/Attack Assessment and NATO's Regional Command (North) Command and Control Architecture and National Defense systems.

DTRA has also conducted assessments on foreign-owned assets. Coordination usually comes through the Executive Secretary to the Secretary of Defense and then to DTRA. DTRA then

---

[23] COL Dennis Baldridge, DTRA, interview to the OUSD (I) CIP Vulnerability Assessment Requirements Team, 30 April 2003.

[24] Except where noted, the source of the information for this methodology is a written and oral interview conducted by the OUSD (I) CIP Vulnerability Assessment Requirements Team with COL Dennis Baldridge, DTRA on 30 April 2003.

coordinates through the U.S. Embassy or Consulate in the host country, then to the foreign installation commander if possible. These types of assessments are conduced in accordance with the requesting organization's rules.

Assessment Teams. Nominally, a BSA team consists of a government team chief (GS 14/15 or active duty O5/6), a mix of 10 to 15 contractors in the technical disciplines, and requisite team leadership and administrative support. Because the team is composed to meet the customer's requirements, DTRA adds additional personnel as needed by the size and complexity of the assessed entity. BSA team core competencies include the following:

- Structural protection and response (including blast effects modeling)
- Information operations (e.g., computer networks, operations security)
- Communications (e.g., voice and data, commercial and military)
- Utility subsystems (e.g., power and HVAC reliability and endurance)
- Emergency response (e.g., fire, damage control, and reconstitution)
- Electromagnetic pulse and radio frequency weapon susceptibility
- Physical security (e.g., AT/FP standards)
- Surveillance operations
- Weapons of mass destruction protection
- Mission operations

DTRA trains and certifies all team members. A typical BSA team will field over 200 worker-years of relevant experience. DTRA can add additional specialists (e.g., medical or explosive ordnance disposal) depending on assessment requirements. BSA team members have security clearances, giving them access to the most sensitive DoD and national information.

Standards and Methodology. Published in FY 2000, the Standard Operating Procedures (SOP) for BSA teams list the DoD and respective industry regulatory and technical references and other sources of assessment standards for each BSA team specialist's functional area or discipline. This edition of the BSA SOP is still current, although DTRA is presently reviewing it for updates. As of July 2003, DTRA had not yet re-published its standards SOP. Although BSA specialists use the SOP assessment checklists and guides, they also rely on their personal knowledge and experience with the assets and with regulatory and technical standards.

The overall BSA process encompasses multiple months. Figure 3.2 illustrates the components of the methodology. To coordinate with the installation/facility commander and staff and brief them on the BSA process, provide an overview of BSA data requirements, agree on the scope of the BSA, obtain information about the organization's mission and critical systems or elements, and address administrative support issues, BSE normally schedules a pre-visit about a month prior to the onsite phase

The BSA team conducts the pre-assessment visit with two team members, normally the team chief and the technical integrator. They give a set of asset information surveys to the installation/facility staff to complete and return to the DTRA before the full team's arrival. Assessors from each discipline use the survey information to determine their focus in the

upcoming assessment. Team members conduct pre-assessment research on the site (e.g., open source and geospatial information data) to prepare for the onsite interviews and information collection.

During the onsite portion of the BSA, team members identify and assess the locations, information and communications networks, equipment, sites, and people who are critical to the mission in order to identify mission vulnerabilities and develop mitigation recommendations. The team collects information through interviews and observations of normal operations. They also review plans and procedures used by the local asset owners to respond to threats, hazards, and warnings.

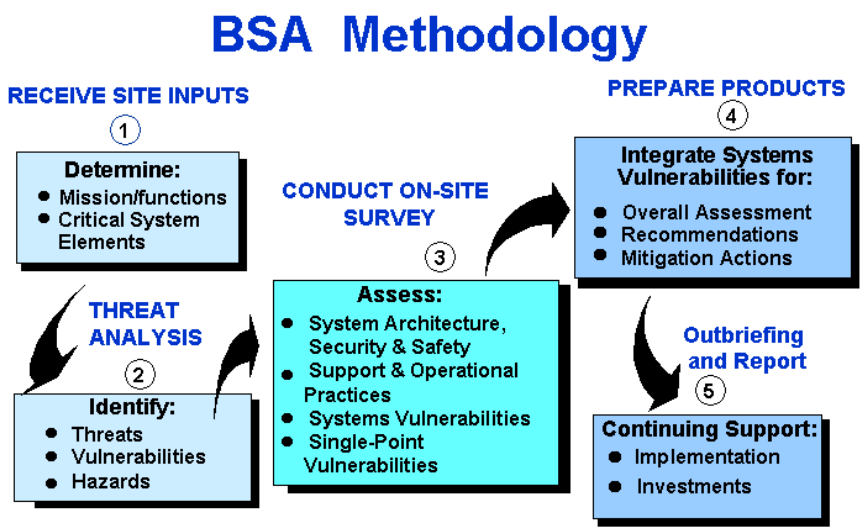

Figure 3.2 – DTRA Balanced Survivability Assessment

BSA teams identify threats from their pre-assessment review of data from law enforcement authorities and agencies, including DIA, CIA, and NSA. "Possible" threats (unconstrained) are considered based on knowledge about capability and observed vulnerabilities; "most likely" threats are considered as a function of capability and history of similar incidents. If requested, the BSA team can call in Surveillance Operations (SO) specialists to simulate "threat" intelligence collection operations. SO-related actions usually take place before the normal onsite assessment. To maintain credibility, the SO team can obtain only installation/facility information that threat collection efforts would normally have available to them, such as information from intrusion, direct observation, Internet searches, or other public sources. These teams contribute their collection efforts to the final report and can participate in BSA team discussions with the sponsoring commander.

The onsite portion of the BSA generally takes two weeks. Because the BSA team is tailored to the customer, the onsite phase can range from one to three weeks, depending on the site's size and complexity. The team will focus on assets identified either as single points of vulnerability (assets that if lost could stop or significantly degrade mission continuity) or as critical single points of vulnerability (assets that if lost would prevent the continuity of the mission). Interdependent supporting infrastructures, originally identified during the pre-assessment site visit, are verified and assessed.

Data Collection, Follow-up, and Final Report. Daily team member observations are captured on a notepad computer. At the end of each onsite day, the BSA team holds an "observation group" session to focus on each discipline. These sessions result in the

identification and prioritization of threats and vulnerabilities as determined by team consensus. DTRA states that prioritization is not determined by formula, and the process is subjective, relying on the significant experience of the team assessors over a more objective process. The team chief and technical integrator lead the team in the discussions and integration/interdependency analyses that take place in these meetings.

The team briefs the installation/facility commander and staff at the end of the onsite phase, summarizing the major findings. The reports are normally classified as secret or higher because of the aggregate information classifications of the assessed site and asset. The classification is determined using the BSA security classification guide and the rules of the assessed site. Security is a primary concern for the BSA team. While onsite, the team conducts its analyses and records information at the installation's Secured Classified Information Facility (SCIF). Team members write their daily and preliminary reports within the SCIF using only the SCIF computers provided by the installation or facility commander.

The BSA team will finish the formal final report within 90 to 120 days of the onsite assessment. Reports, which take both paper and CD-ROM formats, are sent to the installation/facility commander. DTRA will retain a few report copies but will normally not release any copies without the installation/facility commander's approval. When requested, DTRA provides continuing support to assist in implementing recommendations or designing and developing new architectures, equipment, processes, or procedures. DTRA does not currently have a way to track a team's recommendations about asset vulnerability remediation, and so cannot verify that an asset owner or the installation/facility mitigated vulnerabilities.

Joint Staff Integrated Vulnerability Assessments (JSIVA)

General Information. JSIVA is a vulnerability-based evaluation of an installation's ability to deter and respond to a terrorist incident. The assessment primarily focuses on determining the susceptibility to attack, from a full range of threats to the security of personnel, family members, and facilities. The information provides a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks.[25]

JSIVA is the most actively used DoD methodology. DTRA conducts JSIVA assessments about 80-100 times per year to support the DoD AT/FP program and DoD-directed special events in support to the National Special Security Events (NSSE) program. DTRA established the JSIVA process in 1997 following the Downing Commission recommendations. The commission investigated the terrorist attack on DoD personnel at the Khobar Towers in Saudi Arabia in 1995. The Chairman of the Joint Chiefs of Staff (CJCS) directed DTRA to establish the JSIVA program based on the commission's recommendations.

JSIVA is an assessment of potential mass casualty/large loss of life events, which could occur at DoD and other Federal installations or sites. JSIVA will normally assess only those sites that will have approximately 20 or more personnel present at any one time. If a critical

[25] Except where noted, the source of the information for this methodology is a written and oral interview conducted
by the OUSD (I) CIP Vulnerability Assessment Requirements Team with selected DTRA staff on 7 May 2003.

infrastructure site or a facility is unoccupied or only minimally occupied, JSIVA will not assess it. DoD facilities are required to have a JSIVA conducted every three years as a part of the DoD AT/FP program. Assessments generally are one week in duration.

While the JSIVA methodology is not primarily a CIP critical asset vulnerability process, it has been used for CIP assessments. When DTRA uses JSIVA for the CIP program, they add other team members to enable them to focus on assessing an installation's critical infrastructure asset vulnerabilities. DTRA normally does not conduct JSIVAs on DoD sites that do not physically reside on a DoD installation. For example, a DoD Finance Center located in a DoD-leased building located in a major city would not normally receive a JSIVA except in a special request.

DTRA conducts JSIVAs at U.S. installations overseas, but not on foreign assets. However, DTRA conducts JSIVAs on foreign-owned asset that are leased to house DoD personnel and assets. DTRA has conducted JSIVAs for non-DoD agencies. JSIVAs are normally conducted on a cost-reimbursable basis. They require authorization from the Assistant Secretary of Defense for Homeland Defense (ASD (HD)) before the start of the assessment. Additionally, they are only conducted if the current JSIVA schedule permits added assessments.

Assessment Teams. Each seven-person team from the Antiterrorism Assessments Division, Combat Support (CS) Directorate, consists of military and civilian specialists. See Figure 3.3 for a diagram of team responsibilities. A terrorist operations specialist looks at current threats and threat levels, the threat assessment process and operations security. The specialist also assesses observations, actions and attack mechanisms that may be employed by terrorist groups. Two security operations specialists collect information through interviews with key physical security and antiterrorism/force protection personnel. They review operational plans, physical/personal protection procedures and security forces manning, training and equipment.

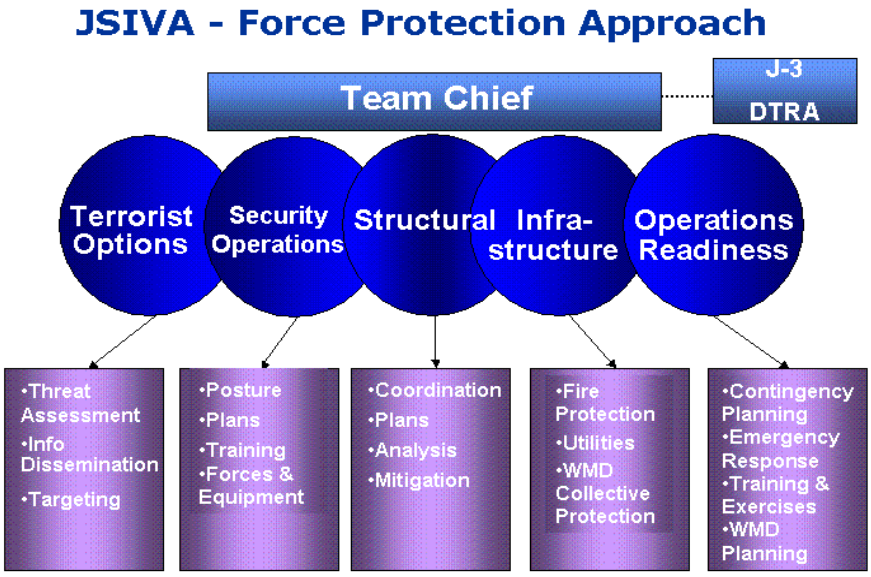

Figure 3.3 – DTRA Joint Staff Integrated Vulnerability Assessment

A structural engineer interfaces with base engineers and planners, surveys selected structures, reviews architectural and structural drawings and performs quantitative analysis of blast effects to establish effective standoff distances. The structural engineer also provides a tutorial on the role engineering plays in the installation's overall force protection posture. An infrastructure engineer focuses on the installation's supporting infrastructure such as water, power, and communications protection against terrorist incidents. The infrastructure engineer also determines if there are any potential single-node points of failure. An emergency management specialist focuses on the installation's preparedness to respond appropriately to a terrorist attack employing explosives,

chemical, biological, radiological, and nuclear weapons. The emergency management specialist also reviews public affairs, medical, emergency operations center, legal, and communications programs.

All team members are required to possess the basic knowledge and/or education degree associated within the team specialty to which they are assigned. Once selected, team members complete a three-phased training curriculum that includes written and practical evaluations. The division chief and functional group leader certify every team member who successfully completes the training curriculum.

Standards and Methodology. The JSIVA team uses DoDI 2000.16, *Antiterrorism Standards* as their main standard for conducting assessments. Additional sources of standards include DoD O-2000-H, *Protection of DoD Personnel and Assets from Acts of Terrorism* and DoDD 5200.8R, *DoD Physical Security Program* for their assessments. DTRA is planning an expansion of the JSIVA scope, to include the addition of Weapons of Mass Destruction as an assessment functional area.

The DTRA JSIVA has a principal focus on terrorist threats from organizations or individuals. There is normally no detailed treatment of other categories of threat. Vulnerabilities are identified based on observed instances of non-compliance with the benchmarks contained in the JSIVA Guidelines, and the collective daily discussions of the assessment team. The team does not prioritize noted vulnerabilities. To prepare for an assessment, the JSIVA team will contact the FBI to obtain specific threat information on the intended assessment site. They use the local law enforcement authorities to give them crime and terrorist information.

The JSIVA does not prioritize vulnerabilities when conducting assessments. DTRA views the installation or facility commander's responsibility to conduct a risk assessment and prioritize the vulnerabilities for mitigation. They do provide the facility with a methodology to accomplish this, which DTRA calls the "CARVER" method for criticality, assessability, recoverability, vulnerability, effect of population, and response.

Data Collection, Follow-up, and Final Report. The JSIVA team members use specific checklists (functional area "Benchmarks" contained in the JSIVA Guidelines) to record and gather data during an assessment. These checklists are designed to adhere to the standards that JSIVA uses to conduct an assessment. The team will also conduct interviews of key personnel at an installation and observe the operations of that facility to gather information. The JSIVA process offers "reach back" for the facilities' staffs through an e-mail help line. Facility or installation Anti Terrorism Officers can send e-mail questions to the DTRA assistance address and a DTRA JSIVA member will respond via e-mail with information assistance to address questions, data information, and or with training materials. JSIVA members have returned to some sites to provide follow-on assistance after an assessment but this is not a standard practice.

The JSIVA team completes a report for each site assessed. This report would be submitted to the installation or facility commander approximately 45 days after the assessment is completed. DTRA generally classifies these reports as CONFIDENTIAL or higher. DTRA considers it the responsibility of the facility or installation commander to prioritize their vulnerabilities and perform risk assessments based on the information in the final report.

DTRA will use the final report as a basis for their next assessment on that facility or installation within next three years.

DTRA maintains the JSIVA reports at their home office and uses the archived reports to develop trends for the current year. On request, DTRA can provide this trend analysis information to other members of the DoD community.

Navy Integrated Vulnerability Assessment (NIVA)

General Information. The Naval Integrated Vulnerability Assessment is an expert third-party or peer review. It is a comprehensive CIP assessment instrument conducted by the Department of the Navy (DON). The Navy Chief Infrastructure Assurance Officer (CIAO) provides the coordination and leadership for synthesizing several existing assessment methodologies. The DON CIAO office collectively refers to these methodologies as the "four pillars" of the NIVA program (see Figure 3.4). The four pillars are the:

- Marine Corps, CNO Integrated Vulnerability Assessment, or DTRA's JSIVA team for Anti-terrorism and Force Protection (IVA AT/FP)
- Marine Corps Enterprise Network (MCEN) or Fleet Information Warfare Center (FIWC) assessment teams for computer network vulnerability
- JPO-STC's IAP team for non-organic and other commercial infrastructure assessments
- DOC CIAO or HQMC consequence management staff team for Continuity of Operations Plans (COOP) and Consequence Management assessments[26]

The NIVA CIP vulnerability assessment process uses the "four pillars" as a baseline for its analysis. NIVA also creates a coordinated assessment process, adds a supply chain and business assessment aspect for Defense industrial base assets, conducts assessments of only "critical"[27] Defense Infrastructure assets, and mandates remediation and follow-up within 120 days. NIVA is intended to be performed at all Navy regions, at other major Navy concentration areas, and at major Marine Corps installations. Occasionally, the Navy will use DTRA's Joint Staff Integrated Vulnerability Assessment (JSIVA) program to conduct the AT/FP portion of their NIVA.

The NIVA is an integrated CIP assessment led by the DON CIAO office. The DON CIAO coordinates the assessments so that all of the "four pillar" assessment organizations are on site at the same time to conduct their assessments within a coordinated assessment plan. The DON CIAO schedules the assessments by Naval region. Beginning with the NIVA programs starting in 2002, the Navy planned to conduct three NIVA assessments per year. Because there are 12 Navy/Marine Corps regions worldwide, approximately one quarter of the Department of the Navy will receive a NIVA every year. As of the end of FY 2003, the Navy has not conducted any overseas NIVA assessments, however, the Navy plans to conduct one in FY 2004.

---

[26] Except where noted, the source of the information for this methodology is a written and oral interview conducted by the OUSD (I) CIP Vulnerability Assessment Requirements Team with Messrs. Neill Robins and David Swindle, of the DON CIO office on 6 May 2003.

[27] "DoD owned or operated cyber and physical assets essential to the execution of the National Military Strategy." See DoDD 3020 (Draft), *Critical Infrastructure Protection (CIP) Program*, 15 October 2003.

Assessment Teams. The NIVA program seeks to coordinate the scheduling of the assessment process to permit all four teams to arrive on the site within a scheduled window to conduct their respective assessments. The DON CIAO office provides a coordination element to lead the team, while other team components include:

- DTRA JSIVA team of 5-7 for AT/FP assessments
- FIWC and/or the MCEN team of 1-3 for computer network assessment
- DON CIO or HQMC consequence management team of 3-7 for COOP and response and recovery planning
- JPO-STC Infrastructure Assurance Program (IAP) team of 3-4 for commercial asset assessment

Overall, team size is determined by the type of installation/facility (either Navy or Marine) and the number of team members necessary to complete the assessment within the two-week assessment period

Standards and Methodology. Each of the assessment teams uses DoD, Federal, and/or technical standards that address their respective team specialty. For example, the DTRA JSIVA and the JPO-STC IAP teams would use those standards previously identified. The computer network assessment teams would use appropriate DoD Information Assurance (IA) and Information Operations (IO) directives and technical specifications. The DON CIAO has developed policies to guide Consequence Management operations based on DoD COOP directives and internal Department of the Navy policies. Together, the four teams rely on an extensive body of standards to guide the assessment.

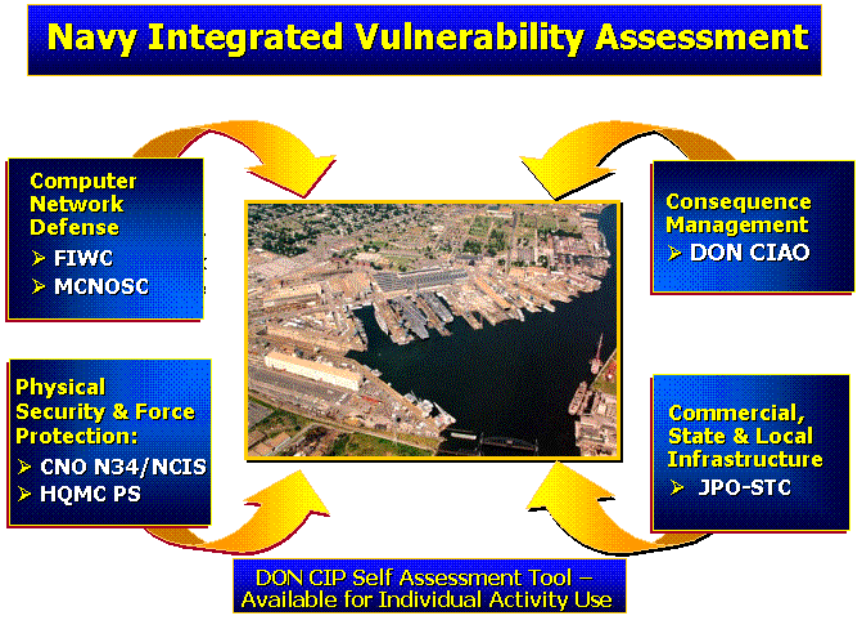

Figure 3.4 – Department of the Navy NIVA Assessment Process

Representatives from the DON CIO, usually two people, conduct a pre-assessment visit to the assessed regional installation/facility. These two individuals explain the NIVA goals, scope and activities, and information requirements from the assessed installation/facility. This information about the installation/facility is sent by the DON CIAO to the respective assessment teams for their pre-assessment review. The DON CIAO coordination team finalizes the schedule for the four assessment teams with both the respective team leaders and with the

staff of the assessed installation/facility. The individual teams decide how many and which personnel to send to conduct the assessment.

Each assessment team conducts their assessment activities within the scheduled timeframe. When two or more teams are on the site, the DON CIAO team coordinates the daily back brief to the installation/facility staff. Following the two-week assessment period, the respective assessment teams prepare their respective reports. The team leaders to the DON CIAO Consequence Management staff forward these reports. This staff analyzes the reports and identifies crosscutting issues. They develop the NIVA final report based on the inputs from the four assessment teams' aggregated findings. There are frequent direct communications between the DON CIAO analysis staff and the team personnel who conducted the assessments.

Data Collection, Follow-up, and Reports. The NIVA final report will normally be completed within 60 days of the time the DON CIAO Consequence Management staff receives the other team's final report. The final classified report is distributed by the DON CIAO to the assessed installation/facility, the regional major commander, and to the other assessment team leaders. The general format includes: introduction, overview of the NIVA, assumptions, details of the four assessment components, and a general summary of findings. The report does not provide remediation recommendations. While the Navy and Marine Corps' asset identification, characteristics, and vulnerabilities are captured in the DON CIAO database (called the Data Management System (DMS)), the NIVA process does not currently have a method to track remediation of vulnerabilities. This database can be accessed and searched by CIAO-approved interested parties and will eventually be distributed over secure systems. Normally, there are no scheduled follow-up visits to the NIVA process unless individually directed by Navy Department leadership.

Common Characteristics Demonstrated

The four vulnerability assessment methodologies described in this section exhibit several important common characteristics that would be desirable in a standardized DoD CIP assessment process.

All the methodologies address several critical CIP assessment interest areas: physical security, operations security, information security and assurance, support of commercial relationships, industrial security, safety, continuity of operations, and remediation recommendations. This wide range of assessment interests would ensure consideration of all the environmental factors that could affect a critical asset's ability to function properly to accomplish mission tasks. A more comprehensive approach taken in assessing vulnerabilities can ensure that most potential vulnerabilities will be detected. Further, the more comprehensive the assessment process, the more adaptable it will be to all types of assets and infrastructure systems.

All the methodologies emphasize best practices using specific standards derived from the Defense Department and using other Federal or related industry technical specifications. Anchoring the assessment process to specific standards makes the process a reliable, repeatable one that provides consistent outcomes. Standards-based assessments require the assessment methodologies to emphasize trained and certified assessment teams. This can also reinforce

that outcomes are reliable and will support the development of valid recommendations for remediation.

All the methodologies use protocols that guide the assessment process. These protocols include pre-assessment information exchange, onsite observations and interviews, use of pre-established checklists for recording data, periodic assessment team back-briefs to the installation or facility commanders or managers, onsite exit briefing, and a final report delivered some 60 to 120 days following the end of the assessment. Standardizing these protocols would lead to a process that, if centrally planned and coordinated, could be used to logically and deliberately prioritize and schedule vulnerability assessments DoD-wide. This could reduce the impact on installation commanders and staffs of performing a number of independent assessments. Not addressed in the five examples in this section are the data elements collected during final report preparation. This should also be addressed in any standard assessment methodology.

All the methodologies provide the facility commander with recommendations for remediation based on the assessment findings. It is essential to note, however, that none of the described processes incorporates any return visits or tracking mechanisms to determine if the recommendations were acted upon or if any remediation was taken to mitigate observed vulnerabilities.

The next two sections will review efforts by the DoD CIP community to identify desirable capabilities and characteristics for the DoD CIP program. While the process of determining desirable attributes began shortly after the start of the DoD CIP program, it is just now reaching the point where specific recommendations have been made and coordinated. The newly organized CIP program office has the task of developing and implementing a centrally managed and resourced assessment program. Their task will be made easier by the extensive analysis and discussion that preceded their current effort.

SECTION 4 – SEEKING A COMMON BASIS FOR A STANDARDIZED CIP VULNERABILITY ASSESSMENT

Is there a common basis for a standard CIP vulnerability assessment process? Can a single vulnerability assessment methodology address all the assessment needs of all the multiple categories for hundreds of critical Defense infrastructure assets? Can several existing assessments be synchronized to meet mission assurance purposes? This section reviews DoD CIP program efforts to address these issues.

From 1999 through 2003, the DoD CIP program management under the OASD (C3I) CIP Directorate oversaw three major projects to determine the basis for common standards in vulnerability assessments: the demonstration project program (1999–2001), the Appendix 16 Pilot Project (2002–2003), and the vulnerability assessment studies (2001–2003).

Since the start of the first of the vulnerability assessment demonstration projects, the DoD CIP community has reviewed and discussed the merits and drawbacks in many of the assessment methodologies, and has sought to determine a basis for common standards in vulnerability assessments. Often these discussions have occurred within the CIP Integration Staff (CIPIS) conferences, during which the feasibility of developing a common set of DoD-wide CIP program vulnerability assessment standards has been considered. The options fall into three general outcomes:

- A new standardize assessment that could be used for all DoD CIP vulnerability assessment purposes,
- The adaptation of one or more of the existing assessment methodologies as the "official" CIP vulnerability assessment, or
- The pooling and collective use of several existing assessment methodologies based on matching the assessment instrument's standards and methods to the infrastructure asset's characteristics and environment.[28]

This range of choices was partly developed based on the CIPIS members aggregated experiences while participating in three major CIP Directorate and Joint Staff projects aimed at understanding the proper role and function of the vulnerability assessment process within the CIP program.

CIP Analysis and Assessment Demonstration Projects

The DoD CIP demonstration projects were the initial efforts of the newly established CIP program to develop a standard process to conduct analysis and assessments of critical Defense infrastructure assets. Using the guidance provided in the 1998 DoD *Critical Infrastructure Protection Plan*, the OASD (C3I) CIP Directorate planned and conducted four demonstration projects beginning in 1999. Working in collaboration with JPO-STC, the CIP Directorate sought to determine the feasibility of developing a standard process for analysis and assessment activities. With a standard process, the CIP Directorate, through JPO-STC,

[28] OASD (C3I) CIP Directorate, *CIP Integration Staff (CIPIS) Meeting Notes*, November-December 2002.

could develop an integrated analysis and assessment report about a given set of infrastructure assets. This report could then generate specific requirements for remediation activities and identify requirements for indications and warning efforts. The CIP Directorate, therefore, had to establish a standard analysis and assessment methodology that would provide a standardized set of integrated inputs into the remaining events of the CIP life cycle model first identified in the DoD CIP Plan.

The demonstration projects started with a primary focus on vulnerability assessments for both Defense and commercial assets. They then progressed to the identification, characterization, and interdependency analysis of critical infrastructure assets. Gradually, they shifted from a focus on Defense installations and their supporting commercial infrastructures to a focus on regional, then operational, mission functions by the Combatant Commands. By December 2001, the demonstration projects started a process that would eventually lead to a formalized CIP analysis and assessment process. Additionally, they started prioritizing mission assurance information to Combatant Commanders and developed an early version of an integrated report that could guide remediation planning.[29]

Tidewater Exercise. The first demonstration project took place in July 1999 in the area of Norfolk, Virginia. This exercise was to be the first major collaboration activity among the CIP Directorate, JPO-STC, a major commercial infrastructure provider, and other DoD CIP components, in this case, the Navy. The purpose for this initial project was to establish ways to identify critical assets, assess their vulnerabilities using DTRA's JSIVA, and identify asset vulnerabilities that would potentially require remediation.

The outcome validated the process and highlighted three assessment lessons learned:

1. Develop specific guidelines for sharing assessment information between commercial infrastructure owners and the Defense Department
2. Develop an analytical process to determine the regional consequences of single critical asset failures
3. Synchronize DTRA's established assessment methods with CIP analysis and assessment goals and requirements to generate desired CIP-relevant information

PACNORWEST. Following the Tidewater exercise, the CIP Directorate coordinated and sponsored the second project in the Puget Sound area. Spanning a six-month period during mid-to-late FY 2000, this demonstration project examined the regional interdependencies of disruptions to critical infrastructures and individual critical assets. It included 20 site assessments by DTRA, the Naval Criminal Investigative Service (NCIS), and JPO-STC. DTRA and NCIS used their respective DoD installation vulnerability assessment methodologies, while JPO-STC used its revised Infrastructure Assurance Program (IAP) Vulnerability Assessment process to assess both DoD and commercial assets. Six participating Defense Infrastructure Sector lead agencies supported JPO-STC in identifying and analyzing critical assets.

The larger regional scope of this project resulted in additional assessment lessons learned:

---

[29] OASD (C3I) CIP Directorate, *A CINC Mission Assurance Critical Infrastructure Protection Demonstration Project Work Plan (Draft),* 21 January 2002.

1. Assign specific analysis and assessment responsibilities to each DoD assessing organization so that appropriate CIP-relevant information is collected.
2. Coordinate assessment schedules and information sharing procedures to avoid unnecessary duplication of effort.
3. Involve all appropriate Defense Infrastructure Sector agencies in the analysis and assessment process to ensure that sector issues or information needs are identified and addressed.
4. Include multiple assessment disciplines such as AT/FP, physical security, personnel security, information security, and operations security in the assessment process because each contains some CIP-relevant information.
5. Design assessments that focus on missions, not just regions or individual installations, to ensure that the effort provides usable information to war-fighting commanders and to identify asset interdependencies.
6. Precede assessments with a mission-to-asset-to-site analysis to ensure that the most appropriate assessment instrument assesses mission-dependent assets.

Malmstrom AFB. The third demonstration project was conducted at a single installation with a single dominant mission. The project focused on a single U.S. Strategic Command (STRATCOM) mission plan at Malmstrom Air Force Base, Montana. The project included the use of three existing vulnerability assessments. Three teams conducted their site assessments from 23 July until 4 August 2000. DTRA conducted BSA and JSIVA assessments, and JPO-STC conducted its IAP assessment. The BSA assessment concentrated on STRATCOM mission-critical command and control facilities, while the JSIVA assessment concentrated on base security of personnel and physical assets. The IAP assessment concentrated on base and local commercial infrastructure assets that support STRATCOM's operational mission. This first CIP mission-focused demonstration project generated several more vulnerability assessment lessons learned:

1. Using multiple vulnerability assessment methodologies to address a CIP assessment process requires prior detailed coordination to identify and determine CIP-specific assessment objectives for each methodology.
2. Detailed pre-assessment coordination with DoD and commercial infrastructure asset owners is necessary to gain appropriate access and to effectively schedule assessment activities.
3. Conducting routine joint assessment team and asset owner information sharing sessions concurrent with the assessment helps ensure continued onsite cooperation, process feedback, and immediate remediation of some identified vulnerabilities.

Rocky Mountain Corridor (RMC). The fourth and final demonstration project was conducted to refine the CIP analysis and assessment process using one of the U.S. Space Command's (SPACECOM) mission plans.[30] Unlike the Malmstrom project, the RMC project involved infrastructure assets dispersed over a regional area. The RMC project was designed to encompass all the aspects of the previous demonstration projects, including:

[30] OASD (C3I) CIP Directorate, *Rocky Mountain Corridor Analysis and Assessment Process Report,* 30 November 2001.

- Analysis and assessment activities,
- A role for appropriate Defense Infrastructure Sector lead agencies,
- Cooperation with other Federal, local government, and commercial organizations,
- Coordination and information sharing among participating organizations, and
- Provision of mission analysis and assessment information to the SPACECOM Commander.

The project focused on SPACECOM's Integrated Tactical Warning and Attack Assessment (ITW/AA) mission, with a planned duration from August 2000 to August 2001. Some planned assessments were not completed by the time of the project report.

The most ambitious of the four demonstration projects, the RMC project had six significant objectives:

1. To identify critical ITW/AA mission tasks, subtasks, and capabilities using JPO-STC and sector analysis teams
2. To identify mission-critical assets using the same teams and identified capabilities
3. To map the assets to the capabilities and to other interdependent assets using the same teams
4. To assess vulnerabilities in the required telecommunications infrastructures of the regional telecommunications providers based on collaboration among JPO-STC, the National Telecommunications and Information Administration (NTIA), and the Office of the Manager - National Communications System (OMNCS)
5. Assess nine installations using DTRA BSA teams and BSA methodology, and incorporate the prototype MIDAS[31] toolset as a part of the vulnerability analysis
6. Develop an analysis and assessment report for SPACECOM that integrates the data and information from multiple project activities

The CIP Directorate decided to terminate the integrated analysis and assessment report because the assessment process was not complete, and DoD and Joint Staff requirements following the events of 11 September 2001 drew JPO-STC and DTRA assets away from the project.

Even without an integrated analysis and assessment report to SPACECOM, the RMC project generated the following useful lessons learned:

1. Existing BSA protocol did not permit automatic assessment information sharing without release from the installation or asset-owning commander, which restrains the access to CIP-relevant information
2. Protecting commercial vulnerability information is a competitive and liability concern to commercial asset owners that must be addressed through national legislative action

[31] Mission Degradation Analysis Support (MIDAS) program is a DTRA effort to develop CIP tools and methods to examine the possible effects on military missions resulting from attacks on supporting infrastructures. Begun in 2000, it is a six-year development project to substantially support the BSA program. For more information, contact the MIDAS program manager: (703) 325-1160, mark.sward@dtra.mil.

3. Lack of an approved, consistent CIP analysis and assessment process leads to incomplete or inconsistent information gathering and reporting

Demonstration Project Contributions to the CIP Vulnerability Assessment Process. These early efforts by the CIP Directorate along with JPO-STC and other CIP components provided an effective beginning to the CIP community's understanding of the dynamics of the CIP assessment process. In 1999 and 2000, the demonstration projects helped the newly organized CIP Directorate and CIP component organizations develop coordination procedures and understand the requirements of the DoD CIP program. The major observations from the projects indicated that the existing assessment methods, which had been independently designed to meet specific organizational requirements, had gaps and redundancies from a DoD-wide CIP program perspective. The assessments focused primarily on specific security issues related to the installation, which did not adequately identify or assess cyber and physical asset vulnerabilities associated with other critical infrastructure asset dependencies and interdependencies. Further, inadequate coordination of assessment schedules and insufficient information sharing hindered DoD-wide CIP program utilization of the information to better understand asset characteristics, interdependencies, and vulnerabilities. The demonstration projects led to the realization within the CIP Directorate and among some of the CIP components that there is a need to develop a standardized analysis and assessment process to address the problems identified in the demonstration projects.

Following the final report from the RMC project, the CIP Directorate terminated the demonstration projects in November 2001. The demonstration projects had adequately shown to the CIP Directorate and Joint Staff the need for a standardized mission assurance analysis and assessment process. The next step was to conduct a pilot test of the analysis and assessment process as a component part of the Joint Operation Planning and Execution System (JOPES). The test vehicle was the development of an Appendix 16 (CIP) to Annex C (operations) to one of U.S. Pacific Command's operational missions.

Developing a Vulnerability Assessment Process for JOPES Mission Planning

In August 2001, the Director of the Joint Staff requested that USPACOM serve as the lead supported Combatant Command for developing the first Joint Operational Planning and Execution System (JOPES) appendix for CIP to an operational plan (OPLAN). Later to be known as the CIP Appendix 16 Pilot Project, USPACOM started the project despite a lack of resources, manpower, and the availability of standard CIP processes and templates. OASD (C3I)'s CIP Directorate received Defense Emergency Response Funds (DERF) in December 2001 as a direct result of the September 11 terrorist attacks. A significant portion of the DERF was forwarded to USPACOM and JPO-STC in late January 2002 for development of the first-ever Combatant Command CIP deliberate plan. The Joint Staff and USPACOM agreed to a 30 April 2003 deadline for completing the CIP Appendix 16 plan. The Joint Staff directed other Combatant Commands to closely monitor PACOM CIP efforts and use USPACOM's CIP Appendix 16 plan as a template for developing their own supporting CIP plans.[32]

[32] OASD (C3I), *Department of Defense FY 2002 Critical Infrastructure Protection Annual Report, U.S. Pacific Command*, 20 January 2003.

Project Guidance. The Joint Staff provided planning guidance to USPACOM, including the following tasks as a part of the CIP Appendix 16 plan:

- Develop a methodology for identifying mission-critical infrastructure assets
- Use existing DoD assessment organizations to conduct CIP assessments to identify physical and cyber vulnerabilities, asset dependencies (both intra- and inter-sector), and single points of failure
- Develop an indications and warning process to monitor the assurance of mission-critical assets
- Develop remediation plans to address vulnerabilities
- Develop infrastructure protection plans, including mitigation plans against the potential loss of a critical asset, response plans to defeat infrastructure threats, and reconstitution plans to restore a critical asset's capability after loss

In April 2002, USPACOM developed a close partnership with JPO-STC, the designated technical integrator for the DoD CIP program and for the Appendix 16 project. The USPACOM/JPO-STC team closely reviewed, and ultimately implemented, a CIP methodology called the Mission Area Analysis (MAA). The MAA is a systematic approach that links Combatant Command missions to infrastructure assets critical to a given OPLAN, contingency plan (CONPLAN), or crisis action plan (CAPLAN). This top-down, mission-focused approach begins by identifying and prioritizing MERs based on a specified plan. MERs are specific Combatant Command or Joint Task Force capabilities essential for guiding the execution of a war-fighting plan. Linked to forces, functions, and tasks, MERs help CIP vulnerability assessment teams to determine high-priority mission-critical assets for assessment.

Appendix 16 Process. The command's MAA began with setting up an operational plan to which the CIP methodology would be applied. Then USPACOM identified mission-supporting MERs at each pre-selected assessment site. Rather than following the previous method of allowing the MAA process to determine assessment site priorities, USPACOM selected the assessment sites and installations before conducting the MAA. This allowed USPACOM to pursue an MAA from the *inside out* rather than *top-to-bottom*.[33] This revision permitted linking the MER to forces and then to the functions and tasks supporting those forces. USPACOM advocated this process as a mature mission analysis and assessment process that could be duplicated by all of USPACOM's subordinate commands as well as by other Combatant Commands for their OPLANs, CONPLANs, and other CIP assessment plans.

As shown in Figure 4.1, when the MAA is finished, the analysis phase is complete and the focus shifts to the assessment phase. USPACOM used its CIP working group to brief the CIP assessment team about the MAA data. The assessment team used the MAA data to determine the scope and focus of the assessment for the highest priority mission-critical assets at designated locations. During 2002–2003, the command used two different but complementary DoD assessments. First, DTRA conducted its BSA, normally a two-week mission-focused assessment at an installation or other designated site. DTRA conducted ten

[33] USPACOM, *OPORD 3020-03 Critical Infrastructure Protection* (Draft), January 2003

of these assessments in the USPACOM operational area. Second, JPO-STC conducted IAP assessments. For the Appendix 16 project, IAP was used to assess both commercial and military asset vulnerabilities and dependencies using an area assessment approach. JPO-STC successfully conducted seven IAP assessments in Alaska, Guam, Hawaii, Japan (including Okinawa), and Korea.

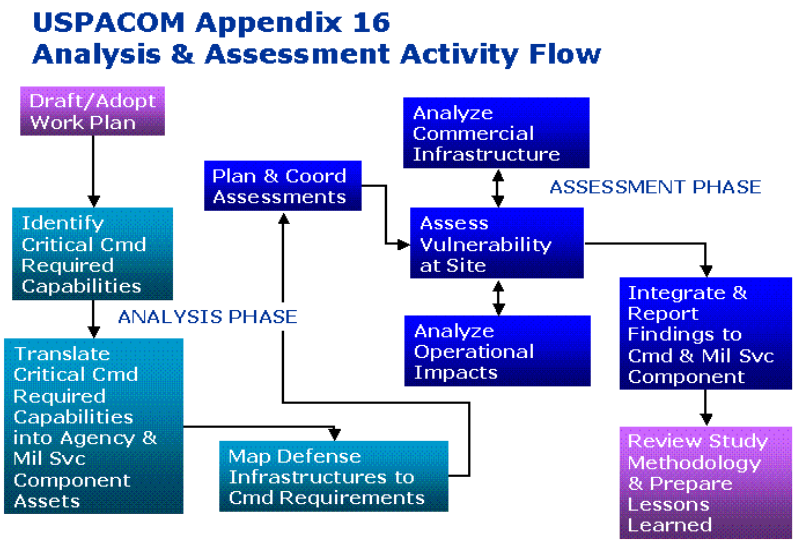

Figure 4.1 – USPACOM Analysis & Assessment Process

Both DTRA and JPO-STC provided final assessment reports directly to the USPACOM J30T AT/CIP Branch. The command reviewed the assessment information, entered the data from these reports into its CIP asset database, and will develop remediation and protection plans for mission-critical assets. At the time of this report, PACOM had not completed all of steps of their 11-step analysis and assessment process (as discussed in Section 2, page 15). As of the conclusion of the step eight ("Conduct Assessment") by the end of April 2003, USPACOM had not yet received all the vulnerability assessment reports needed to complete step nine ("Write Report") for all seventeen of the assessment sites. However, enough information was gathered for USPACOM to evaluate the entire process.

Project Outputs. The Appendix 16 project had three principal outcomes:

1. There is now a methodology for identifying mission-critical infrastructure assets. For the first time, the Combatant Commands have a demonstrated methodology to address mission assurance of critical assets as a part of the JOPES planning process.
2. USPACOM developed a model Appendix 16 in support of a specific command operational plan. This model plan provides instructions regarding mission assurance actions to the command and provides a model for future Appendix 16 development for subsequent USPACOM plans.
3. USPACOM developed its OPORD 3020, *Critical Infrastructure Protection*, as planning guidance to the command's staff and subordinate commanders for both ongoing and future plans and operations. OPORD 3020 is USPACOM's "Theater Infrastructure Protection Plan" for establishing a template for "operationalizing" the command's CIP program. The plan outlines how USPACOM incorporates the six CIP life cycle events into planning and execution among the command's headquarters directorates, military components, and sub-unified commands. The document also includes ten infrastructure-specific theater sector plans for assuring individual sector assets and systems critical to USPACOM missions. It describes the important CIP processes and includes flowcharts detailing the complex asset analysis and assessment functions.

This joint USPACOM and JPO-STC document provides valuable information for the development of similar plans by the other Combatant Commands.

USPACOM-Recommended Assessment Process Improvements. In both the general assessment process and in the DTRA and JPO-STC assessment reports, the USPACOM CIP staff identified several significant shortfalls that should be addressed in future Combatant Command assessments and in any standard DoD CIP vulnerability assessment process:[34]

- Assessment standards – There must be DoD policy guidance for establishing an approved and resourced vulnerability assessment program and standards.
- Assessment scheduling – The Combatant Commander, not the installation commander, should schedule assessments. The Combatant Commander is able to identify critical asset interdependencies, asset contribution to MERs, mission impact analysis from asset disruption, and use of vulnerability information to better guide mission-specific remediation.
- Terminology and data lexicon – According to USPACOM, definition is less of an issue than the processes associated with a term. Terms like assessment should include collection requirements based on the MER, asset tasks, asset functions, asset direct or indirect support organizations, and asset granularity (description, owner, location, loss consequence, vulnerabilities, and mitigation/response/reconstitution options).
- Report receipt requirements – Current final assessment reports are not timely nor in a form easily converted to asset information databases. This result in long delays in obtaining important data (2–10 months) and expensive staff-hour costs in collecting data from multi-page written reports and inserting the data into the command's asset database.
- Information sharing – Current DTRA rules restrict assessment report distribution to the installation/facility requesting the assessment. USACOM recommends that the Combatant Commander be another principal recipient so that selected components of the assessment report can be shared within the command and with the Defense Infrastructure Sector points of contact, and extracted into the command database for further asset information sharing (with appropriate access security controls).
- Link assessment data collection to the CIP database – The command's CIP asset database should be the end state for the information output developed during each assessment. Each assessment should have standard data elements that can be entered on data sheets to support automated data correction.
- Coordination between assessment teams and the Combatant Command – In the absence of a standard DoD CIP vulnerability assessment, the Combatant Commands must conduct pre-assessment coordination with the participating assessment agencies to ensure that their assessments are tailored to the command's requirements. USPACOM recommends that the coordination include team members from the selected assessed installation(s) and the Military Service, and includes asset inter/intra-dependency mapping.

[34] Interview summary between the USPACOM Joint Staff CIP points of contact and the OUSD (I) CIP Vulnerability Assessment Requirements Team, 19 May 2003.

Appendix 16 Project's Impact on the DoD CIP Vulnerability Assessment Process. Since the release of the USPACOM project report and draft OPORD 3020 in April 2003, the Joint Staff has reviewed the methodology and its application to the other Combatant Commands. As of this date (October 2003), the Joint Staff has not officially announced its findings and recommendations regarding the implementation of USPACOM Appendix 16 by the other commands. Officially stated project benefits to the DoD CIP assessment process will occur following the Joint Staff's official approval and adoption of the process.

In the meantime, discussions at the CIPIS meetings have indicated concern about the cost and complexity of the overall joint USPACOM and JPO-STC Appendix 16 methodology. Despite this criticism, most of the Combatant Command CIP staffs state that they have begun using the Appendix 16 model to start their analysis and assessment processes for OPLAN critical asset assurance.[35] They assert that the Appendix 16 project provides a relevant overall methodology that addresses Combatant Command interests for mission critical infrastructure asset assurance. Most important for developing a CIP vulnerability assessment process, the Appendix 16 Project provided considerable experience in applying previous DoD vulnerability assessment methodologies to specific DoD CIP assessment requirements.

As part of its development, the Appendix 16 project used the experiences from the previous demonstration projects to emphasize the importance of pre-assessment coordination among the assessment agencies, the assessed installation and facility's military and public/private asset owners, and the command's stakeholders. The project model stressed interagency collaboration to achieve confidence for information sharing and timely access for asset assessment. Additionally, the USPACOM staff provided numerous briefings to the CIP components, at CIPIS meetings and elsewhere, keeping the community informed about the process and obtaining feedback. Several CIP component organizations (e.g., Transportation, Logistics, Intelligence/Surveillance/Reconnaissance (ISR), and Global Information Grid/Command and Control (GIG/C2) sectors) were actively engaged in the process.

The USPACOM assessment process also stressed pre-assessment asset identification, characterization, and mapping to other inter- and intra-dependent assets as critical. Finally, the project model revealed that the outcome of the assessment process must be transferable to the command's asset database. This is important because it will permit the asset's characteristics, links to specific units, mission functions, mission tasks, vulnerabilities, and interdependencies to be clearly identifiable to mission planners, asset owners, and other CIP component elements, such as the Defense Infrastructure Sector lead agencies.

The lessons learned from the PACOM and JPO-STC Appendix 16 methodology were important sources of information about development of a standard CIP vulnerability assessment program.

Deliberate DoD Studies of the CIP Vulnerability Assessment Process

Concurrent with the RMC demonstration project and the USPACOM Appendix 16 project, the DoD CIP Directorate conducted two additional studies. Both studies sought to

[35] OUSD (I), *CIPIS Notes*, 16 April and 15 May 2003.

understand how vulnerability assessment can be utilized in the DoD CIP program and where there may be a basis for a standardized CIP assessment.

CIP Directorate/Joint Staff Integrated Vulnerability Assessment Integrated Process Team (IVA/IPT). The IVA/IPT conducted a study from January through May 2001. The study was designed to perform a detailed analysis of current DoD methodologies that have some CIP application. The analysis aimed to determine their assessment standards, protocols, scheduling, oversight and management, information collection and handling, and information sharing policies. Following the analysis, the IVA/IPT was to address seven project tasks that together would recommend an integrated CIP vulnerability assessment process that could integrate the most appropriate aspects from the existing assessment methodologies.[36]

Early in the analysis, the IVA/IPT team determined that it would not have the time to address all seven tasks in its charter. Instead, the team addressed three questions, each question including elements from one or more of the study's seven tasks. The three questions and the team's findings are shown in Figure 4.2.

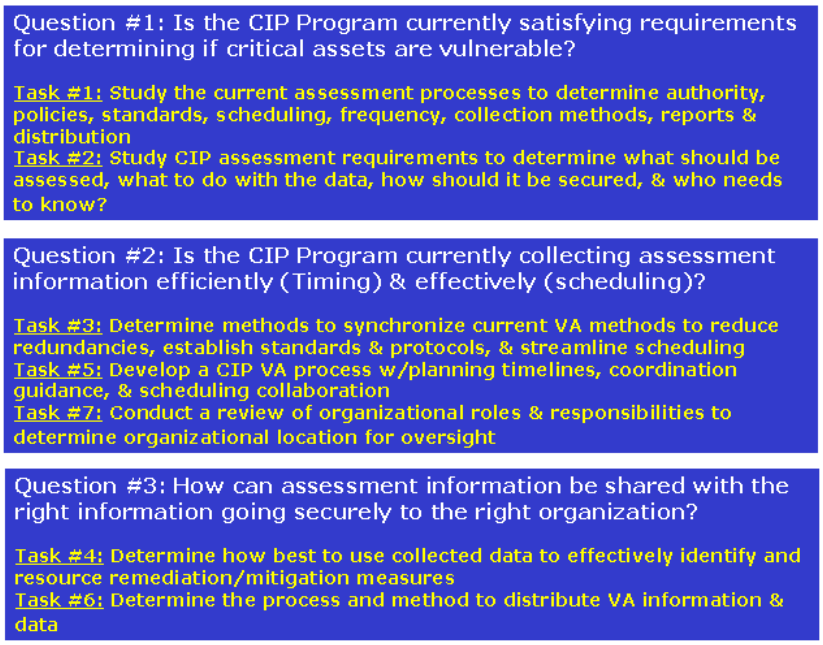

Figure 4.2 – IVA IPT Project Research Questions w/ Project Tasks

The study identified 22 CIP-relevant DoD vulnerability assessment methodologies. The assessment matrix (Appendix D) consisted of a text table that described the characterization (e.g., focus/purpose, duration, standards) of each assessment. This table was discussed earlier in Section 3 of this report.

The study concluded that there is a DoD CIP requirement for a "coordinated, CIP vulnerability assessment process that supports CINC (Combatant Command) operational mission assurance." The study did not state the need for a separate, stand-alone CIP assessment. Rather, it found the need to develop protocols that would allow using existing assessments in a collaborative and integrated manner to address a range of CIP assessment and information-sharing requirements. The IVA/IPT report supplements this conclusion with three recommendations:

[36] OASD (C3I) and Joint Staff (J-5), *OSD and Joint Staff Integrated Vulnerability Assessment Integrated Process Team, Final Report*, 31 July 2002.

1. DoD should establish a clear and comprehensive policy to govern a CIP analysis and assessment process. The policy should address standard processes to identify, prioritize, and select assets for assessment, assessment coordination and scheduling, unique considerations for commercial assets, information sharing specifics (e.g., classification and proprietary information protection), and DoD CIP component roles and responsibilities. As part of this recommendation, the report specifically mentioned establishing a technical working group to study and recommend a process to integrate existing vulnerability assessments, using the JSIVA scheduling process as a model.
2. DoD should develop a common set of vulnerability assessment protocols that will support standard and repeatable outputs, relevant information sharing among specific CIP component members, and a CIP risk-management decision template. The technical working group would develop the protocols. In addition, the working group would select a self-assessment tool that can be used for asset owner's internal risk-management decisions, develop the JPO-STC's IAP assessment methodology for CIP-related commercial asset assessments, and examine DTRA's BSA methodology as a model for mission-critical asset assessments. As a part of this task, the working group would develop a resourcing baseline to support the development and validation of the CIP assessment process.
3. DoD should establish a vulnerability assessment information clearinghouse, with appropriate security safeguards to support information sharing and assessment scheduling. To implement this recommendation, the IVA/IPT specified that DoD should develop an electronic method to report and catalog all DoD CIP-related assessment information for rapid accessibility using standard search tools and linkages. Also specified was that DoD select an appropriate assessment organization as the executive agent for CIP vulnerability assessment. The executive agent would be responsible for scheduling, reviewing protocols, and maintaining data management tools.

The IVA/IPT study clearly started the process for DoD's CIP management to develop an integrated and collaborative process to address a standardized approach for vulnerability assessments. However, it left to a yet-to-be-determined working group with the responsibility for actually implementing the study's recommendations. It proposed an aggressive schedule that assumed the working group would be available by 1 June 2002 and would complete all components of the three recommendations by the end of October 2002. That did not happen. Formation of the working group was delayed by one year. One significant factor for the delay was the limited availability of funds to create and operate the working group. Another factor was the CIP Directorate's desire to evaluate the outcome of the RMC demonstration project. The project was scheduled to end in August 2001, but the final report was not available until November 2001.

The delay in the implementing the IVA/IVP report's recommendations did not appear to adversely effect ongoing CIP assessment activities because the lack of adequate funds meant that few CIP-related assessments were taking place outside of the demonstration projects. This changed after the terrorist attacks of September 11. Mission assurance asset identification and vulnerability assessments became a high priority for the DoD staff, Military Departments, and Combatant Commands. Further, funding in the form of the Defense Emergency Response Fund (DERF) enabled the CIP program to conduct multiple

assessments. By mid-2002, the number of assessments in progress in behalf of the Appendix 16 project and by the Defense Infrastructure Sector lead agencies led the CIP Directorate to announce the formation of a new working group.[37]

OSD/Joint Staff Vulnerability Assessment Technical Working Group (VATWG). From late July until December 2002, the VATWG developed recommendations, specific products, and processes necessary to implement the IVA/IPT reports previously described third recommendation. The working group was not tasked to develop DoD CIP policy for analysis and assessment, or to develop common vulnerability assessment protocols as cited in the IVA IPT report's first and second recommendations. Instead, the VATWG was charged to determine if actions in the third recommendation were still valid. If so, it was authorized to implement those recommendations. The VATWG plan specified that the group would receive guidance and direction from the Vulnerability Assessment Steering Committee, consisting of OASD (C3I) CIP Directorate, Deputy Under Secretary of Defense (Policy Support), and the Joint Staff (J-5/Global).[38] Unfortunately, due to competing requirements, the steering committee was not formed and the OASD (C3I) CIP Director provided all guidance and directions to the VATWG.

The VATWG charter tasked the team to accomplish the following three tasks. The working group's recommendations and the outcomes are described for each task.

Task 1 - Develop a catalog of vulnerability assessments (not vulnerability information). The categories of assessment information within the catalog included type of assessments, who conducts the assessments, the scope or focus of the assessment, what assets were assessed, and who owns the assessment report.

Recommendation/Outcome. The VATWG selected JPO-STC as the catalog's steward and developer. The catalog will be a 13-item data spreadsheet that records all vulnerability assessments since FY 1999. Figure 4.3 lists the categories for the data fields. Initially, the catalog would be unclassified (FOUO), released on a CD-ROM, and would be continuously updated. JPO-STC will make future reviews to upgrade information and determine possible reclassification to higher security levels depending on the aggregated level of information (new content and classification) that could be placed in the catalog as the process matures.

Task 2 – Develop a process to ensure that assessment information is shared with CIP component organizations that can use the information. The process will have appropriate safeguards; a means to facilitate correcting identified deficiencies, and the provision of process oversight.

Recommendation/Outcome. The VATWG developed a policy statement that would establish an information sharing process and a Vulnerability Assessment Information Adjudication Board to handle conflicts related to requesting and releasing CIP-related vulnerability assessment information. The process would operate on a "need-to-know" basis under which CIP component organizations and other DoD or federal agencies with appropriate classified access authority could request information about DoD vulnerability assessment report. Request denials could generate an appeal to the Adjudication Board,

---

[37] OASD (C3I) memorandum, *Establishment of a Vulnerability Assessment Technical Working Group*, 12 June 2002.

[38] OASD (C3I) and Joint Staff (J-5), *OSD/Joint Staff Vulnerability Assessment Technical Working Group, Final Report*, December 2002.

which would review the validity of both the request and denial and offer a judgment. The board would consist of members (no rank/grade or position specified) from the Joint Staff J-3 and J-5, OASD (C3I), OASD (SOLIC), and ODUSD (Policy Support). The policy did not address the board's enforcement authority over information request denials from installation commanders and other asset owners within the Military departments.

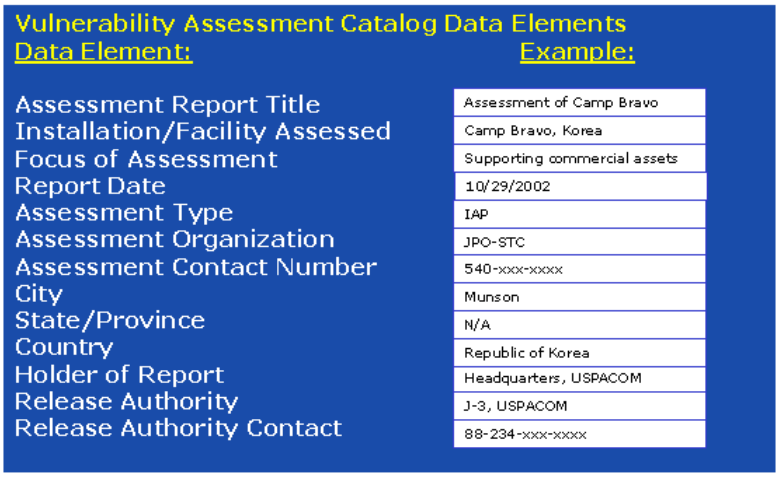

Figure 4.3 – VATWG Recommended VA Catalog Information Elements

Task 3 – Develop a recommendation to the VA Steering Committee about establishing an Office of Primary Responsibility (OPR) for coordinating the vulnerability assessment process within DoD and serving as the DoD assessment point of contact to non-DoD agencies. If the VATWG recommends an ORP, then the group should recommend ORP roles, responsibilities, authority, and OPR organizational site.

Recommendation/Outcome. The VATWG recommended establishing an OPR, but said that a follow-on effort should develop the details about roles, responsibilities, and the designated organization. The new OASD (HD) agency, then a part of the OUSD (Policy), was named as the point of contact for external, non-DoD agencies requesting assessment information. The lack of a recommendation was due to insufficient time in the working group's charter.

The only long-term impact of this study was the development of a vulnerability assessment catalog that identifies the information categories in Figure 4.3. JPO-STC completed the work in August 2003 and began issuing the unclassified (FOUO) CD-ROMs in September 2003. The working group, however, did not make recommendations about establishing an adjudication board nor did they establish a recommendation about approving and issuing an information sharing policy. Further, the working group did not complete its recommendation for selecting a DoD vulnerability assessment program OPR. All these activities appear to have been delayed due to the DoD organizational changes that took place from March to September 2003. Under the changes, management of the DoD CIP program was transferred from OASD (C3I), through OUSD (I), to OASD (HD).

Impact of DoD Studies for Developing a Standardized CIP Vulnerability Assessment Process. The IVA/IPT and VATWG studies did not result in the development of or a recommendation for a detailed concept of a CIP-specific vulnerability assessment process. The IVA/IPT study recommended developing a DoD policy a common set of vulnerability assessment protocols that would support standard and repeatable outputs, relevant information sharing, and a template for risk management decision-making. However, the study recommended that a follow-on working group accomplish the task. The VATWG formed the following year chose not to accomplish the policy and development tasks. Instead, it elected to produce the IVA/IPT-recommended assessment catalog that would be

the record and description of past assessments. Additionally, the VATWG did not recommend establishing an assessment information sharing process, nor did it select and define the roles and responsibilities of a DoD vulnerability assessment OPR.

Did These Projects Establish a Common Basis for a Standardized CIP Vulnerability Assessment?

Collectively, the demonstration projects and the IVA/IPT and VATWG studies did not establish a common basis for a developing standardized CIP vulnerability assessment. On one hand, their findings do clearly indicate that the current use of multiple, independently scheduled assessment methodologies is not achieving the CIP strategy for vulnerability assessments. On the other hand, these same findings also indicate where there are general areas of agreement for establishing a common basis for a standardized DoD CIP assessment process. A summary of major findings and recommendation from these projects can be found in Annex B.

The demonstration projects identified the necessity of a deliberate pre-assessment activity. Such a step is essential to synchronize the distinct protocols of several cooperating assessment methodologies within an assessment mix oriented to a given set of infrastructure assets and supporting a given Combatant Command mission. While, the individual assessment methodologies separately specify their own pre-assessment requirements, the demonstration projects, particularly the RMC project, illustrate the value of synchronizing the pre-assessment activities of each. Identified pre-assessment activities included:

- An asset mapping process to link "mission-to-asset-to-site" to ensure that the most important mission critical assets are assessed
- A determination of information sharing protocols and the scheduling of assessment sequences
- The determination of desired objectives for the collective assessment process

Lessons learned from the joint USPACOM and JPO-STC Appendix 16 Pilot Project validated the pre-assessment findings from the demonstration projects and identified two major areas for assessment standardization:

- The effectiveness of tailoring specific assessment characteristics from the DTRA's BSA and JSIVA assessments and the JPO-STC IAP assessment to the most appropriate mission critical assets
- The importance of converting assessment report outputs into electronic data to enter into a Command's asset database to clearly link asset identity, characteristics, interdependencies, vulnerabilities, and remediation options into a properly secure but accessible site for mission planners, asset owners, and other CIP Component organizations

After an extensive review of the available range of DoD assessment methodologies, the two OASD (C3I) vulnerability assessment study teams verified that the current assessment process remains fundamentally uncoordinated, non-integrated, and redundant. The VATWG found that the current system places undue burden on critical asset owners, who

must sort through potentially conflicting vulnerability remediation recommendations from multiple program-specific assessment reports.

To reemphasize two important developments: the two study teams did uncover and document general knowledge about the characteristics of available DoD assessments, and their efforts produced the release of a vulnerability assessment catalog listing the type, frequency of use, assessment focus, and other minimum essential information.

SECTION 5 – DOD ACTIVITIES LEADING TOWARD THE DEVELOPMENT OF A STANDARDIZED CIP VULNERABILITY ASSESSMENT

Section 4 of this report identified deficiencies in the current DoD vulnerability assessment process while also delineating areas of agreement in finding a common basis for a standardized DoD CIP process. At the conclusion of the projects and studies that lasted from 1999 to 2003, a vulnerability assessment requirement team, led by the OASD (C3I) Deputy CIP Director, took up the task of actually developing the required capabilities, characteristics, and design for a standardized CIP vulnerability assessment program. Therefore, this section will address a question that is essential at this point: What is the plan to develop a standardized CIP vulnerability assessment process?

Resources for answering this question come from work done by the CIP Vulnerability Assessment Requirements team, which was set up by the previous Deputy CIP Director of OASD (C3I) in October 2002. Two documents developed by the team, *CIP Vulnerability Assessment Requirements Statement*, and *CIP Vulnerability Assessment Program Transition Document*; provide the basic concept for a standardized CIP assessment process. During the reorganization of the DoD structure during 2003, the responsibilities for this effort were first transferred to OUSD (I)/Security & Information Operations (S&IO), then later to OASD Homeland Defense (HD). Within OASD (HD), the new CIP Director assigned the task to the newly organized Defense Program Office for Mission Assurance (DPO-MA). The program office prepared its vision document, *DoD CIP Full Spectrum Vulnerability Assessment Program*, to state its goals and objectives for the program. While the DPO-MA planners have just started to determine the scope and direction of a DoD-wide assessment process, they have a legacy with the JPO-STC IAP assessment program and have been actively engaged in the standardized CIP assessment concept since the days of the demonstration projects.

Developing Requirements for a DoD CIP Vulnerability Assessment

The OASD (C3I) CIP Directorate's vulnerability assessment requirement statement was published in January 2003. The statement reflected the work done concurrent with the preparation of VATWG final report. The CIP Directorate did not task agency-member VATWG to address the development of a common set of vulnerability assessment protocols as was recommended by the IVA/IPT in July 2002. That task went to a contractor team established by the Deputy CIP Director. This team reviewed all previous DoD analyses of the vulnerability assessment process, reviewed current policies and regulations, conducted interviews with DoD assessment agencies, and developed a requirement document and assessment program design.

New Assessment Objective and Requirement Statements. The requirement team elaborated on the general guidance in the CIP strategy by providing an objective and a requirement statement for a distinctive CIP vulnerability assessment program.

Objective: "*The primary objective of the CIP VA is to provide senior DoD leadership and Combatant Commanders with a quantifiable measure of the vulnerabilities of mission-essential critical assets that will support the identification of the risks to military capabilities and operations*."[39]

The key rationale of this CIP assessment objective is as follows:

- To provide asset owners the quantifiable basis to allocate scarce resources in the remediation decisions
- To reduce critical asset vulnerabilities
- To reduce the risk that asset disruptions could degrade or prevent the execution of Combatant Command missions

Establishing a consistent, repeatable and quantifiable DoD-wide vulnerability assessment process would correct the CIP Directorate's four-year-long observations about the uncoordinated, non-integrated, and redundant character of existing assessment efforts. Further, an accepted, uniform DoD-wide process can be a more transferable methodology for other Federal agencies and the Defense Industrial Base to use. The emphasis in this objective statement is similar to that in the CIP strategy. Unlike the CIP Strategy, however, the new objective does not identify the role of self-assessments, if any, within the vulnerability assessment process. Presumably, self-assessments would remain an asset owner's tool for determining local threats, hazards, and vulnerabilities—independent of other mission dependencies and interdependencies.

Requirement: "*Combatant Commanders, Military Services and Defense Agencies require a Critical Infrastructure Protection Vulnerability Assessment (CIP VA) of the critical assets upon which they rely. The assessments should be conducted annually, or at the frequency of change in the critical assets' supporting infrastructure, or upon a change in mission that requires support from the critical assets, whichever occurs sooner*."[40]

The CIP Directorate required the team to identify the potential CIP assessment's vulnerability components (e.g., physical and cyber assets, and personnel geographical vulnerabilities) and review the asset's supporting components. Supporting components would include infrastructure assets located at other supporting DoD CONUS/OCONUS sites and those among the commercial system, within the defense industrial base, and at foreign overseas/host nation sites.

Required Capabilities and Characteristics. The requirement statement lists and explains the required capabilities for a CIP vulnerability assessment and its corresponding characteristics. Figure 5.1 arranges the two lists in a diagram to show possible relationships among seven stated capabilities and twelve characteristics.

The proposed list of capabilities and characteristics seeks to resolve identified weaknesses in the current CIP assessment process while retaining the desired improvements reflected in the Navy's NIVA program, in the JPO-STC IAP program, and in aspects of DTRA's JSIVA and BSA programs. The proposed DoD CIP vulnerability assessment concept aims to reduce the total number of independent assessment activities at any one installation or facility by having the program be both comprehensive and integrated. It is comprehensive in its ability

[39] OASD (C3I), *Critical Infrastructure Protection Vulnerability Assessment Requirements Statement*, January 2003
[40] Op. Cit.

to address a wide range of potential threat-induced vulnerabilities related to force protection, antiterrorism, physical security, operations security, information security and assurance, on-base and off-base government and commercial dependencies, and industrial security. It is integrated by leveraging the best practices and key assessment protocols of existing DoD programs, which combine well-qualified, independent assessment teams with a standards-based, quantifiable and repeatable process that provides consistent outcomes and reliability over time. The outcome would be a proposed program that would better prioritize and schedule assessments and support asset owner decisions for remediation identified vulnerabilities.

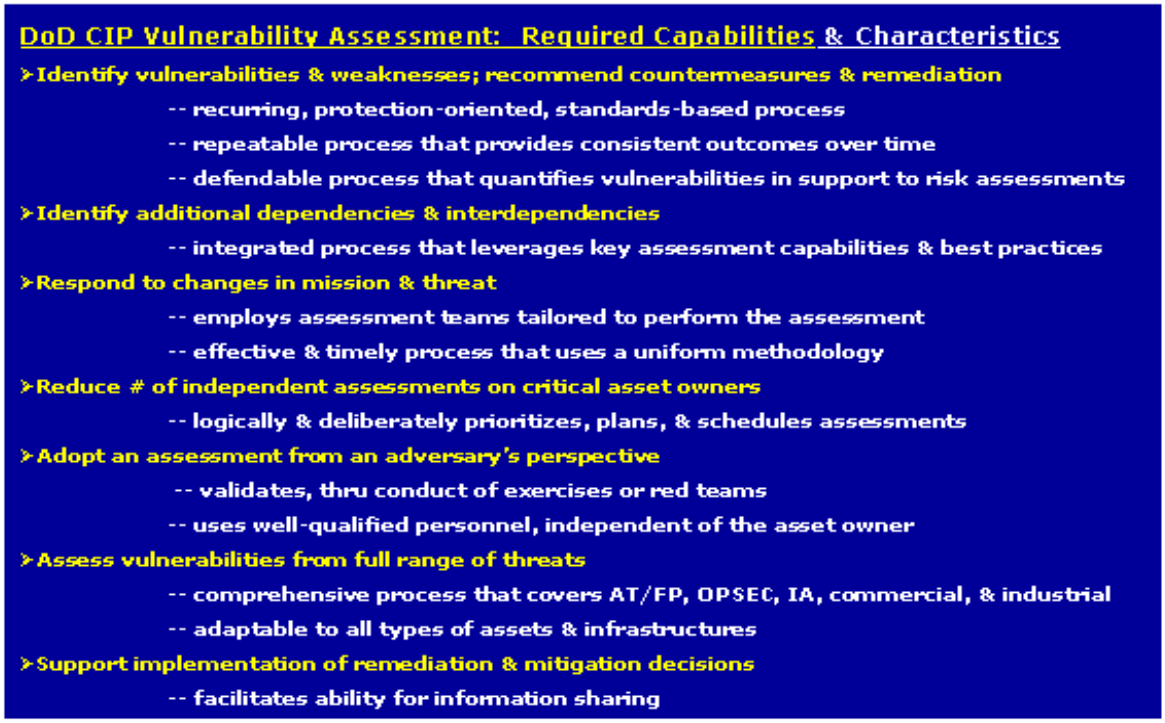

Figure 5.1 – VA Requirements Team's Recommended CIP VA Capabilities & Characteristics

The requirement team distributed the proposals for review and comment among selected CIP component organizations. Based on the feedback received, the team revised the requirement statement, and then used the information in a CIP-Directorate-proposed program concept document, which was published in June 2003.

Proposed Design for a DoD CIP Vulnerability Assessment Program. The CIP Directorate developed a concept document that addressed the design elements for a standard DoD CIP assessment program.[41] The team completed work on this project during the period of DoD headquarters reorganization, when the reorganization eliminated the OASD (C3I) organization and transferred the CIP Directorate to the Under Secretary of Defense for Intelligence (OUSD (I)). The concept document restated the characteristics of the program and added program tasks, specific areas of interest, protocols, and guidance for

[41] OUSD (S&IO), *Critical Infrastructure Protection Vulnerability Assessment Program Transition Document* (Working Papers), 6 June 2003.

implementation. The document's stated purpose was to "…define the practice within the Department of Defense for conducting vulnerability assessments of critical infrastructure assets." The program office stated that in adopting a DoD-wide, comprehensive, integrated, and sustainable CIP vulnerability assessment process would achieve the following benefits for DoD:

- "Provide adequate coverage of vulnerabilities associated with the critical DoD infrastructure assets, especially in those areas of the defense agency activities, defense industrial base, and other commercial infrastructure, and OCONUS/host nation infrastructures and assets
- Address all the protection elements of a critical asset, and address a full range of assets (both cyber and physical)
- Identify for commanders the full range of asset vulnerabilities associated with end-to-end operational dependency across all sectors
- Provide a higher confidence in prioritizing remediation actions
- Provide the basis for validated infrastructure assurance resource requirements in the PPBS cycle"

These benefits address the perceived problems of the multiple current assessment processes, where the "…assessments tend to highlight potential installation-oriented vulnerabilities but do not identify or assess vulnerabilities associated with critical infrastructure assets or their interdependencies." Current assessments "…do not assess a full range of assets (e.g., physical and cyber), and …do not result in an integrated product or report containing actionable material that decision makers can use."

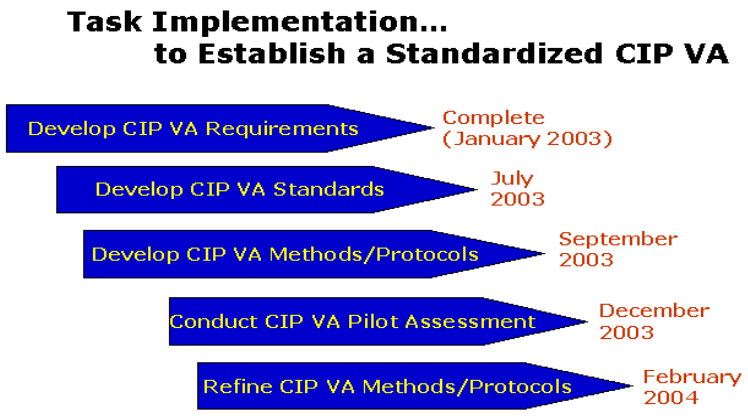

Figure 5.2 – VA requirement Team Recommended CIP VA Implementation Timeline

To guide the process for a proposed implementation in FY 2004, the concept document identified five tasks with associated target completion dates, as shown in Figure 5.2.

Building on the requirements document, specific sets of standards would be developed for each category, addressing a broad range of objective security assessment standards for physical and cyber, DoD and supporting non-DoD assets. In addition, a standard process for assessing critical assets, associated infrastructures, and interdependency-related single points of failure would be developed as a second phase of the standards task. The diagram in Figure 5.3 lists the categories for which the program office would develop the standards and shows examples of asset components addressed by the process. The precise methods and protocols used in the assessment would be the next

tasks to be developed. Finally, the assessment methodology would be tested by the program office in a series of pilot assessments, with feedback and lessons learned applied to revising and refining the assessment methodology.

Areas of Interest	Examples
Identify physical vulnerabilities & weaknesses; recommend countermeasures & remediation	Access, Security, Materials, Construction, Environmental control
Identify cyber vulnerabilities & weaknesses; recommend countermeasures & remediation	Computer systems, Environmental control, OPSEC, INFOSEC
Identify supporting systems & networks vulnerabilities & weaknesses; recommend countermeasures & remediation	Transportation, Telecommunications, Utilities, Energy, Water, Food
Identify supporting personnel vulnerabilities & weaknesses; recommend countermeasures & remediation	Key personnel, organizations, e-mail repositories
Identify supporting commercial vulnerabilities & weaknesses; recommend countermeasures & remediation	Contract support, supply sources, support services
Identify supporting response & contingency plans & weaknesses; recommend countermeasures & remediation	COOP, response, Evacuation, Recovery, Safety, Training

Figure 5.3 – VA Requirements Team Recommended CIP VA Areas of Interest

The concept document proposed both short-term and long-term implementation plans. In the short-term, DoD would leverage existing assessment programs to establish a repeatable, consistent vulnerability assessment process. This process would be similar to the Navy's NIVA program: centralized funding, scheduling and control, deployment of trained assessors currently assigned to existing assessment teams but trained in the new CIP protocols and standards, integrated data collection, report preparation, and data storage in a central CIP database for information-sharing and tracking. In the long-term, the proposal recommends a new program budget line for consistent funding support, new program staff (civilian/contractor/military) skilled and certified in the assessment standards, and continuation of central scheduling and control.

Any actions taken to implement this particular standardized CIP assessment concept ended when the DoD CIP management function transferred from OUSD (I) CIP Directorate to OASD (HD) CIP Director in September 2003. Beyond development of the requirement statement and the concept document, no other significant progress was made during the transition period from June 2003 until September 2003. Efforts until that point, however, were significant in their scope for developing a comprehensive approach to improve the existing and multiple, but narrowly focused, assessment methods. The requirement team's approach was based on the experience gained by the OASD (C3I) CIP Directorate's four-year involvement in monitoring hundreds of CIP-related vulnerability assessments, both as part of deliberate Directorate-sponsored projects and in assessments separately sponsored by other organizations. The changes in CIP management prevented detailed coordination of the concept documents with the major CIP community stakeholders to obtain their feedback and willingness to collaborate in the standardization process. It is uncertain how successful this proposed transformation of the CIP vulnerability assessment process would be or to determine where there would be collective agreement for a standardized CIP assessment process.

Planning for a CIP Full Spectrum Vulnerability Assessment (FSVA) Program.

On 3 September 2003, the Deputy Secretary of Defense officially transferred responsibility for DoD CIP program management from OUSD (I) to OASD (HD). The new CIP program management now has the following responsibility for vulnerability assessments:

"*Ensure the Department develops and uses analytical standards and procedures to permit effective, DoD-wide, infrastructure support analysis and assessments. Ensure the Department has the analytical tools necessary to provide the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the DoD Components with assessments providing the status of critical infrastructure assets*."[42]

To assist the ASD (HD) to perform this responsibility and others, the Deputy Secretary of Defense directed the ASD (HD) to establish a program office to maintain and administer the DoD CIP program. The ASD (HD) established a new CIP Director, who in turn assigned the new program office with specific vulnerability assessment tasks to:

- "Establish, coordinate and maintain a critical infrastructure vulnerability and special technology vulnerability assessment process, including protocols, reporting criteria, data repository and information sharing guidelines
- Coordinate CIP-related site surveys and vulnerability assessments with the Joint Staff, Combatant Commands, and the Military Services and Defense Agencies
- Assist the DoD CIP Director in oversight and approval of CIP assessment scheduling and prioritization, through coordination and leadership of scheduling conferences"[43]

With this authorization, the new CIP Director and the new program office, Defense Program Office for Mission Assurance (DPO-MA), have the authority to establish centralized control over a DoD CIP vulnerability assessment program.

New Assessment Program Concept. In the FSVA concept document, the DPO-MA defines the new program as follows:

"A CIP FSVA is a capability that will comprehensively evaluate the vulnerabilities of critical physical and cyber assets essential to mobilize, deploy, and sustain U.S. Military operations. This capability will address a full range of areas, including physical security, personnel security, force protection, force projection, day-to-day operations, information security, and information assurance assets in support of mission requirements. Critical assets that will be assessed may include those of the DoD, the U.S. commercial/private sector, foreign commercial/private sector, and host nations."[44]

The DPO-MA's FSVA concept is very similar to the concept developed by the OASD (C3I) CIP Directorate's Vulnerability Assessment Requirement team. Both concepts stress the need for a comprehensive assessment that covers a wide range of assessment categories for critical DoD infrastructure assets and their supporting DoD and non-DoD infrastructures, the categories also being essential for DoD missions and not just critical for the function of a DoD installation or facility. Both concepts seek to achieve measurable, quantitative vulnerability data using standardized processes and qualified assessors focused on the range

---

[42] DepSecDef, *Realignment of Critical Infrastructure Protection Oversight to the Assistant Secretary of Defense for Homeland Defense*, 3 September 2003.
[43] OASD (HD), *Functional Responsibilities Document (FRD)*, 10 September 2003
[44] DPO-MA, *Department of Defense Critical Infrastructure Protection Full Spectrum Vulnerability Assessment Program* (Draft)(FOUO), 16 October 2003.

of asset dependencies and interdependencies whose disruption or loss can significantly affect mission consequences.

The DPO-MA office should be able to rapidly develop its vulnerability assessment concept because the office was formed from JPO-STC, which has had four years of experience with DoD CIP analysis and assessment activities. These activities include involvement with the demonstration projects, the USPACOM Appendix 16 Pilot Project, and application of the IAP assessment process. This extensive connection to DoD CIP vulnerability assessments and the DoD assessment community gives the aggregated JPO-STC and DPO-MA staff a knowledgeable position from which to establish a comprehensive and integrated CIP assessment program. The current small cadre within the DPO-MA would be augmented by proposed authorized positions, which the concept document identifies as the CIP FSVA "Program Coordinators." These individuals would develop and administer the established FSVA program. The responsibilities planned for the coordinators are as follows:

- Support the development of clear and comprehensive DoD policy for the CIP FSVA program
- Develop a DoD CIP FSVA program management plan
- Develop DoD CIP FSVA requirements, assessment standards, and protocols
- Coordinate with the existing DoD assessment program offices to integrate program characteristics and capabilities as needed and appropriate to support a short-term, interim CIP FSVA program
- Develop a CIP FSVA training and certification program
- Develop a CIP FSVA user's guide
- Develop, implement, and manage a database capable of recording and archiving asset vulnerability data, tracking remediation progress, and sharing vulnerability assessment lessons learned
- Coordinate the conduct of all DoD CIP FSVA program assessments
- Track all reported CIP-related vulnerabilities and associated remediation efforts

FSVA Program Elements. The FSVA program concept includes four major elements.

1. Program coordinators. The coordinators will not only establish the program but will also sustain the program through administrative support for skills training and certification, database management, tracking remediation efforts, and program review and revisions. These individuals will help institutionalize the program by establishing policies, standards, quality control, and routine actions.

2. Scope of assessments. The assessment teams will address an extensive range of assessment perspectives as a part of the methodology they will adopt. Figure 5.4 lists the 14 assessment areas that give this assessment concept its "full spectrum" character. Normally, the program office will not assess all of these perspectives for all the installations and facilities associated with the command mission or infrastructure sector. Nevertheless, having this capability will give the FSVA program more capabilities than any of its DoD predecessors. Achieving this capability in the short term will require integrating far more DoD assessment team assets than attempted in the past. To accomplish this, the many CIP

component stakeholders will likely accept the FSVA concept only after the establishment of agreed-upon DoD assessment policies, a program management plan, and an acceptable set of assessment standards and protocols.

3. Database policies and procedures. The third major element is the establishment of policies and procedures for capturing and inputting extensive vulnerability assessment data into a centralized CIP infrastructure asset database. JPO-STC has sought to develop a central DoD CIP database since late 2002. As a part of its Integrated Data Collection and Analysis System (IDCAS) concept, JPO-STC is developing a capability for a real-time collaborative analysis and planning system for Defense infrastructure assets. Its principal goal is to support DoD-wide needs for securely storing information about mission-related critical assets, dependency paths, operational analysis, and vulnerability and risk assessment. [45]

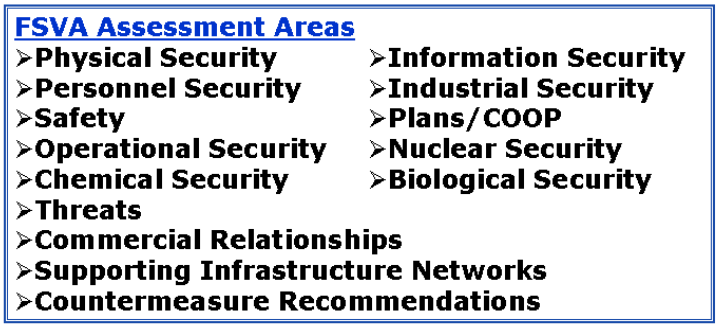

Figure 5.4 – FSVA Program Proposed Assessment Areas

JPO-STC specifically developed this project to meet a strategic area of emphasis in the DoD CIP Strategy's information architecture. The program office would enter FSVA data into this central system, and the DPO-MA would develop input criteria, output requirements, and performance standards. Input criteria are the major information elements (see Figure 5.5) that are used for gathering pre-assessment information and preparing the assessment team. The output requirements specify the assessment products that DoD CIP vulnerability assessors must provide to satisfy the DoD CIP FSVA reporting requirements.

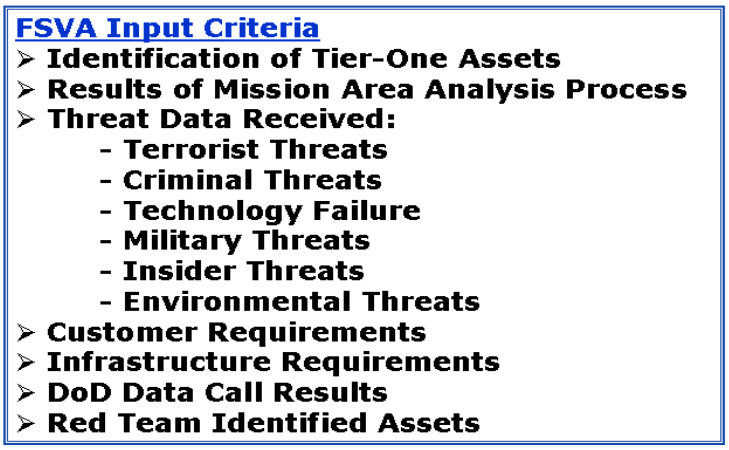

Figure 5.5 – FSVA Program Proposed Initial Data Inputs

Output requirements include report, data element, and after-action requirements. The data gathered during the assessment would support the identification of risks to military capabilities and operations, and assist in deliberate and crisis-action planning. The FSVA process would standardize the data collection elements required to support CIP objectives and accommodate mission assurance and planning. The key data elements will be derived from the electronic version of the final

[45] JPO-STC, *Critical Infrastructure Protection Database Architecture Description and Needs (Version 1.1)*, 17 March 2003.

assessment report, which includes approximately 45 data element categories in its proposed form.

4. Training and certification. The fourth major element is an instructional emphasis aimed at acquiring trained and experienced subject-matter experts who are knowledgeable about CIP concepts and policies and about the associated vulnerability assessment process and standards. The FSVA program plans to integrate teams from several different DoD assessment programs. To make sure that these team members are skilled in the FSVA program's areas of emphasis and can meet the full range of requirements and performance standards associated with the FSVA program, the DPO-MA assessment coordinators would develop a CIP FSVA training program. Upon completing this required training, personnel would apply to the program office for certification to perform FSVA assessments. DPO-MA will be responsible for establishing the certification criteria and granting CIP FSVA certification. Certification will permit supporting organizations and agencies to receive program funds to conduct FSVA assessments to support the CIP vulnerability program. Certification will also obligate supporting organizations and agencies to adhere to CIP FSVA program requirements, policies, and standards when performing CIP vulnerability assessments.

5. Consensus building. The next most critical step will be developing consensus among the assessment stakeholder community. If approved, the DPO-MA CIP vulnerability assessment concept provides both threats and opportunities to the aggregate stakeholders. One threat is that some of the assessment agencies could have functions and associated budgets transferred from their agencies to DPO-MA, if not in the short-term then in the long-term. This threat could be mitigated and turned to opportunity by having dually certified team members for both the CIP assessment process and the agency's stand-alone process. The DoD could gain by decreasing the aggregate number of assessment activities involving DoD installations. Some rationalization of the current, multi-agency assessment process by integrating several assessments into the CIP assessment process could leverage manpower and funding savings. As of yet, however, no cost-benefit analysis associated with either the former OASD (C3I) or the current DPO-MA concept proposals has been released. Therefore, DPO-MA must carefully develop both the subjective and objective merits of a DoD CIP vulnerability assessment program to gain both DoD funding and stakeholder support.

Summary of the Plan. The purpose of the proposed DPO-MA CIP vulnerability assessment program is to develop the policies and standards for an effective DoD-wide approach to assessing critical infrastructure vulnerabilities, as well as complement the DoD CIP analysis process that identifies critical infrastructure assets. The program would provide senior DoD leadership and Combatant Commanders with quantifiable measures to judge the vulnerabilities of mission-essential critical assets that will support the identification of the risks to military capabilities and operations. The fully developed DPO-MA CIP FSVA program would contain the following elements:

- Comprehensive DoD CIP assessment policy and associated program instruction,
- DoD CIP FSVA program management plan,
- Established, and periodically updated, DoD CIP FSVA standards and protocols,
- DoD CIP FSVA training and certification program,

- DoD CIP FSVA program user's guide,
- Database management process to record FSVA data to the DoD CIP asset database, and
- Efforts to record asset vulnerability and track associated remediation

The DPO-MA concept reflects four years of experience gained by JPO-STC members through their participation in the previous CIP vulnerability assessment process. The JPO-STC IAP assessment process was specifically developed to support a CIP analysis and assessment process. Further, JPO-STC has used the IAP process in numerous combined and stand-alone assessment activities supporting the demonstration projects and particularly USPACOM's analysis and assessment program, a key component to its Appendix 16 process. Further, JPO-STC collaborated with the Defense Infrastructure Sector lead points of contact and with some of the CIP functional agencies to address infrastructure sector assessment issues and vulnerabilities. With this previous experience, JPO-STC's knowledge transfer to DPO-MA provides a credible basis for the proposed concepts and proposals.

As OASD (HD) and DPO-MA staff presents their CIP assessment concept to the DoD leadership and CIP component stakeholders, they will obtain feedback, including critical comments and recommendations. While complete agreement may not be required to implement the program, the concept presentation process will generate valuable information about where success can be achieved.

S UMMARY

This report addressed the experiences gained during a series of DoD CIP program activities that influenced the current DoD CIP management to seek to develop a Defense-wide approach to assess both non-DoD and DoD mission-critical infrastructure vulnerabilities. The paper organized the information around five questions. These questions encompassed the intent of the CIP assessment process, its scope, the assessment applications most frequently used, the experience in determining CIP-relevant assessment characteristics, and current standardization plans. The responses below to each of these questions provide summarized information that can help one understand the past and current efforts to achieve an effective CIP assessment process.

What is the concept of Department of Defense (DoD) CIP vulnerability assessment?

To understand the DoD CIP assessment concept is to understand the component elements within the policy definition for the term "vulnerability assessment." As defined within DoDI 3020, it is "The process of determining the susceptibility of critical assets, associated infrastructures, or interdependency related single points of failure to adverse conditions." The DoD definition of vulnerability assessment requires the understanding of four concepts – asset susceptibility to adverse conditions, associated infrastructures dependencies, asset infrastructure interdependencies, and single points of failure.

Asset susceptibility is a function of its vulnerability to certain types of threats or hazards. Vulnerability can best be understood by citing the definition from the current draft of DoDD 3020: "The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment." Therefore, asset susceptibility can have two indicators: asset characteristics, which describe the asset mission, tasks, functions, and physical or cyber properties, and asset threats, which are the types of adverse environment activities that can adversely affect asset characteristics.

Associated infrastructures dependencies are those supporting infrastructure assets within the same infrastructure. They are an inherent part of the asset's infrastructure system. Interdependencies are other external infrastructure support systems and assets, such as energy and telecommunications infrastructures, that permit the critical asset to perform its task. Each of these associated infrastructures will have their own characteristics and threats that assessors must consider in an assessment.

Single points of failure are unique infrastructure characteristics, which have unique assets that if lost would stop or significantly degrade mission continuity. Infrastructures with single points of failure do not have other, redundant assets that can perform the same task or function.

An earlier concept for vulnerability assessment was based on the original guidance from risk management practice as stated in the 1998 DoD CIP Plan and from the Critical Asset Assurance Program (CAAP). This guidance envisioned a program, which would determine

critical assets that have known vulnerabilities combined with known threat exposure. From this analysis, the CAAP process would develop vulnerability metrics that base the remediation process on established and reliable criticality and vulnerability standards. However, the DoD CIP community could not agree as to the appropriate standards to transition the guidance from the CIP Plan and CAAP into an operational assessment process.

In summary, the DoD concept of a vulnerability assessment consists of a set of subordinate concepts that form a component part of an overall CIP risk management process.

How does the vulnerability assessment process contribute to the DoD CIP program?

The DoD CIP strategy established vital vulnerability assessment activities as a component part of the analysis and assessment process. Vulnerability assessments are essential in identifying infrastructure asset vulnerabilities and generating remediation options. Under the DoD CIP strategy, a fundamental part of the CIP program requires conducting comprehensive and tailored CIP vulnerability assessments on both scenario-independent and scenario-dependent critical infrastructure assets only *after* identifying, validating, and prioritizing vulnerability assessment requirements. This way, DoD can preserve scarce vulnerability assessment resources and skills for the most important assets.

The goal of CIP vulnerability assessments is to achieve greater fidelity of information for the senior DoD leadership and Combatant Commanders to use in assessing the risks to critical assets and, consequently, to military capabilities and operations. Additionally, CIP vulnerability assessments would provide infrastructure asset owners with the ability to support vulnerability remediation and mitigation plans, decisions, and resource allocation. These assessments will also support the implementation of mitigation activities to reduce or minimize the operational impact of exploited vulnerabilities. An equally important output of the assessment process is the information generated for developing operational risk management protocols.

What are the characteristics of the vulnerability assessment methodologies commonly used in the DoD CIP program?

Previous studies under the OASD (C3I) CIP Directorate identified 22 DoD vulnerability assessments that had CIP relevance and shared some common characteristics. The four vulnerability assessment methodologies summarized in Section 3 (Integrated Assurance Program, Joint Staff Integrated Vulnerability Assessments, Balanced Survivability Assessment, and the Navy/Marine Corps Integrated Vulnerability Assessment) shared the most common characteristics.

First, all the methodologies address several areas of critical CIP assessment interest: physical security, operations security, information security and assurance, support of commercial relationships, industrial security, safety, continuity of operations, and remediation recommendations. This wide range of assessment interests will eventually permit assessors to consider most of the environmental factors that affect a critical asset's ability to function properly to accomplish mission tasks. Combining these multiple areas into a more comprehensive approach to assessing vulnerabilities will ensure that the majority of the potential vulnerabilities would be detected. Further, the more comprehensive the

assessment process, the more adaptable, flexible, and responsive it will be to all types of assets and infrastructure systems.

Second, emphasis placed on specific standards derived from DoD and other Federal or related industry technical specifications placed their emphasis on best practices. This experience also indicates that anchoring an assessment process to specific standards makes the process a reliable, repeatable one that can provide consistent outcomes. The process becomes reliable because the assessment is more objectively based on using established standards. Reliability permits repeatability, and so the process can be repeated within different infrastructure environments. Consistent outcomes using a reliable and repeatable process also permit subsequent reassessments to accurately measure the effectiveness of applied remediation.

Third, the aggregated characteristics included a set of assessment protocols to guide the assessment process: pre-assessment information exchange, onsite observations and interviews, a pre-established checklist for recording data, periodic assessment team back-briefs to the installation or facility commanders or managers, onsite exit briefing, and a final report delivered some 60 -120 days following the end of the assessment. Standardizing these protocols could lead to a process that, if centrally planned and coordinated, would logically and deliberately prioritize and schedule DoD-wide vulnerability assessments. This could reduce the impact on installation commanders and staffs of a number of uncoordinated assessments.

Fourth, the four assessment teams universally provide the installation or facility commander with recommendations for remediation activities based on specific assessment findings. The feedback process not only addresses specific vulnerabilities, but also exchanges best practices within the DoD CIP community. Not as common within the four assessment methodologies described in this report was the protocol that incorporates return visits or tracking mechanisms to determine if the recommendations were acted upon or if any remediation was taken to mitigate observed vulnerabilities.

Is there a common basis for a standard DoD CIP vulnerability assessment process?

The three major groups of projects reviewed in Section 4 identified multiple points that could become the common basis for a standardized CIP assessment. Annex B lists these points. The points fall within four general categories of requirements:

- Requirement for specific DoD CIP vulnerability assessment policy
- Requirement for a DoD-wide vulnerability assessment program management
- Requirement to synchronize the characteristics and capabilities of the most appropriate existing assessment programs into a uniform set of assessment standards and protocols that can address a full range of CIP infrastructure asset (both DoD and non-DoD) assurance requirements
- Requirement for an assessment information/data sharing process for recording and storing asset vulnerability data, sharing vulnerability lessons learned, and tracking remediation activities

The key points of the three major groups of projects can be summarized as follows:

- The Demonstration Projects identified the necessity of a deliberate pre-assessment activity to synchronize the distinct protocols of several cooperating assessment methodologies within an assessment mix oriented on a given set of infrastructure assets supporting a given Combatant Command mission. While separately, the individual assessment methodologies had their own specified pre-assessment requirements, the Demonstration Projects, particularly the RMC project, demonstrated the value synchronizing the pre-assessment activities of each.
- The vulnerability assessment lessons learned from the joint PACOM and JPO-STC Appendix 16 Pilot Project validated the pre-assessment findings from the Demonstration Projects and identified two major areas for assessment standardization:
  - First, the pilot project demonstrated the effectiveness of tailoring specific assessment characteristics of the DTRA BSA and JSIVA, and the JPO-STC IAP assessment to the most appropriate mission critical assets
  - Second, the pilot project emphasized the importance of the conversion of assessment report outputs into electronic data elements to be entered into a Command's asset database to clearly link asset identity, characteristics, interdependencies, vulnerabilities, and remediation options into a properly secure, but accessible site for mission planners, asset owners, and other interested CIP Component organizations.
- The two OASD (C3I) vulnerability assessment study teams verified that the current assessment process remains fundamentally uncoordinated, non-integrated, and redundant. Therefore, the recommendations included establishment of specific DoD policy for vulnerability assessments, creation of an integrated CIP assessment process that "leverages the best practices" of existing assessments, and establishment of information sharing processes with requisite levels of security classification.

What is the plan to develop a standardized DoD CIP vulnerability assessment process?

The proposed DPO-MA CIP vulnerability assessment program will develop the policies and standards for a comprehensive DoD-wide approach for assessing critical infrastructure vulnerabilities. The program will complement the DoD CIP analysis process that identifies critical infrastructure assets. It is expected to provide senior DoD leadership and Combatant Commanders with quantifiable measures to judge the vulnerabilities of mission-essential critical assets and therefore support the identification of the risks to military capabilities and operations. The fully developed DPO-MA CIP FSVA program would contain the following elements:

- Comprehensive DoD CIP assessment policy and associated program instruction
- DoD CIP FSVA Program management Plan
- Established, and periodically updated, DoD CIP FSVA standards and protocols
- DoD CIP FSVA training and certification program
- DoD CIP FSVA program User's Guide
- Database management process to record FSVA data to the DoD CIP asset database

- Record asset vulnerability and track associated remediation efforts

The FSVA program concept has incorporated the numerous lessons learned and best practices identified by the investigative projects discussed in Section 4 and Annex B. As of October 2003, the DPO-MA started the process of collaborating with both assessor and assessed organizations to determine the program elements, which will achieve concept acceptance and program success.

ANNEX A – TABLE OF DOD VULNERABILITY ASSESSMENT METHODOLOGIES AS CITED IN THE JPO-STC VULNERABILITY ASSESSMENT CATALOG (2003)

Assessment	Description	Assessment Agency	Sources for Standards & Protocols	#Of Reports Cited (1999-2002)
Air Force Vulnerability Assessment (AFVA)	Focused assessment of the antiterrorism and force protection practices and procedures to mitigate and remove vulnerabilities at worldwide Air Force activity locations	The Air Force Security Forces Center (AFSFC)	DTRA's AT/FP guidelines	0
Air Force Hospital Services Inspection (AF-HIS)	Evaluates the ability of particular medical units and their performance of their functions under various peacetime or combat scenarios.	The US Air Force Headquarters and Major Command Surgeon General Staffs	Air Force Surgeon General staff guidelines	0
Balanced Survivability Assessment (BSA)	Examines the vulnerabilities of an organization's mission to a broad spectrum of threats including those posed by natural or man-made events including, for example, fire, terrorist, WMD, or information attacks that will result in the disruption of mission essential systems, operations, or the requisite supporting infrastructure. The assessments are a multi-disciplinary, performance-based approach and that develops mitigations to any identified vulnerabilities to enhance mission assurance.	Defense Threat Reduction Agency (DTRA)	DoD AT/FP, security, IO/IA, OPSEC, and structural engineering industry technical and procedural guidelines, directives, and policies	63
Chief of Naval Operations Integrated Vulnerability Assessment (IVA)	Utilizes scenarios to measure the ability of a military activity to compensate after the effects of degradation on their mission and/or function, including terrorist attack, and their ability to make the necessary adjustments to return to mission readiness.	The Office of the Chief of Naval Operations (OPNAV N34 AT Program Directorate)	DoD and CNO guidelines, directives, and policies	0
Defense Logistics Agency Vulnerability Assessment (DLAVA)	Identifies force protection and supporting infrastructure vulnerabilities at worldwide Defense Logistics activity locations utilizing a structured format technique.	Defense Logistics Agency (DLA) Command Security Office, with US Army Corps of Engineers (USACE)	DoD, USACE, DoS, and DoJ AT/FP and IA guidelines, directives, and policies	7
Defense Security Service Arms, Ammunition, and	Assesses contractor effectiveness in the protection of munitions. Identifies vulnerabilities and recommends remediation measures in the manufacturing, storage, and	Defense Security Service (DSS) and/or the Bureau of Alcohol, Tobacco and Firearms	DoD, DSS, and BATF guidelines, directives, and policies	0

Assessment	Description	Assessment Agency	Sources for Standards & Protocols	#Of Reports Cited (1999-2002)
Explosives Security Support (DSS AA&ESS)	transportation of military procured munitions and explosives.	(BATF)		
Defense Security Service National Industrial Security Program (DSS NISP)	Assesses the effectiveness of cleared contractors in meeting the National Industrial Security Program (NISP) standards of performance in three areas: security systems, security education, and security awareness programs.	Defense Security Service (DSS)	DoD and DSS guidelines, directives, and policies	0
Information Assurance Readiness Review (IARR)	Evaluates the Information Security (INFOSEC) plans and compliances of an activity, installation, or facility.	Defense Information Systems Agency (DISA)	DoD and DISA guidelines, directives, and policies	3
Information Assurance Vulnerability Assessment (DISA IAVA)	Identifies Information Assurance program vulnerability and weaknesses, and whether reporting requirements are being met on DoD installations and facilities. The report is a tool to assist the Chairman, JCS to determine priorities in addressing IA vulnerabilities	Defense Information Systems Agency/Command, Control, Communications, and Computer Systems Directorate of the Joint Staff (DISA/J6)	DoD and CJCS guidelines, directives, and policies	0
Joint Program Office Infrastructure Assurance Program and Mission Operation Dependency (JPO IAP – MOD)	Integrated approach to the characterization of supportive commercial infrastructures and identification of critical assets, the identification of operational dependencies and supporting sites, and the assessment of operational impacts	Joint Program Office for Special Technology Countermeasures (JPO-STC)	JPO-STC developed guidelines and appropriate industry technical standards	130
Joint Staff Integrated Vulnerability Assessments (JSIVA)	Focus on the vulnerability assessment of the anti-terrorism/force protection practices and procedures to mitigate and remove vulnerabilities at worldwide military activity locations	Defense Threat Reduction Agency (DTRA)	DoD antiterrorism, physical and personal security guidelines, directives, and policies, and structural engineering industry technical standards	347
Marine Corps Integrated Vulnerability Assessment	Utilizes on-site interviews and observation during exercise scenarios to measure the ability of an activity or installation to	Headquarters Marine Corps (HQMC)	DoD, Marine Corps, and DTRA guidelines,	5

Assessment	Description	Assessment Agency	Sources for Standards & Protocols	#Of Reports Cited (1999-2002)
(MCIVA)	compensate after the effects of a terrorist attack and make the necessary adjustments to conduct its mission.		policies, and directives	
Naval Integrated Vulnerability Assessment (NIVA)	Comprehensive CIP assessment instrument under DON CIAO coordination and leadership synthesizing several existing assessment protocols. Includes: infrastructure asset vulnerabilities, continuity of operations plans and preparedness assessments, assessments for computer network vulnerability, and non-organic and other commercial infrastructure assessments. The Navy cyclically conducts NIVA at all Navy Regions or other major Navy concentration areas, and at major Marine Corps Installations.	Integrated assessment teams from: Chief of Naval Operations (CNO), Headquarters, Marine Corps (HQMC), and Joint Program Office for Special Technology Countermeasures (JPO-STC)	DoD, CNO, HQMC, and JPO-STC guidelines, directives, policies, and industry technical standards	1
National Security Agency Information Systems Security (INFOSEC) Assessment	The identification of mission critical information, systems, risks management and countermeasure requirements to ensure information security.	National Security Agency (NSA), governmental agencies, and selected contractors	DoD and NSA guidelines, policies, and directives (i.e., NSA INFOSEC Assessment methodology)	0
National Security Agency Operational Network Evaluations (NSA ONE)	Assessment process where assessment teams work directly with network administrators to diagnose, penetrate, and test operational computer networks for the DoD, the Intelligence Community, and other federal government agencies to identify network vulnerabilities and recommend countermeasures.	National Security Agency (NSA)	DoD and NSA guidelines, policies, and directives	0
National Security Agency Red Team (NSA Red Team)	Assessment process that engages in exploitive attempts to compromise U. S. government computers to evaluate network defenses and assess operational preparedness of Defense Information Operations.	The National Security Agency (NSA) and NSA trained assessment teams	DoD and NSA guidelines, policies, and directives, and NSA Red team Rules of Engagement	0
Risk Assessment Methodology for Dams (RAM-D)	Risk assessment methodology to identify effective means of countering the potential threat to the security of the nation's dams. Provides information to support effective risk-reduction decisions by dam management. Process includes a threat assessment, consequence	United States Army Corps of Engineers (USACE)	*"Field Manual and Training Guide"* developed by Sandia National Laboratories to guide assessment	305

Assessment	Description	Assessment Agency	Sources for Standards & Protocols	#Of Reports Cited (1999-2002)
	assessment, and a security effectiveness evaluation.		process with checksheets and worksheets	
Secret Internet Protocol Router Network Compliance Reviews (SIPRNETCR)	Assessments to ensure trust relationship among users by examining user enclaves.	Defense Information Systems Agency (DISA)	DoD security directives and policies, and automated assessment tools	0
Transportation Infrastructure Criticality and Vulnerability (TRICAV)	Assessments to examine the impact of the loss or impairment of domestic transportation infrastructure upon the deployment of military assets, making recommendation for remediation to the predicted conditions.	United States Transportation Command (USTRANSCOM) and Military Traffic Management Command Transportation Engineering Agency (MTMCTEA)	DoD and USTRANSCOM guidelines, policies/ directives, DoD OPLANs and TPFDDs, and engineering and technical documents	0

ANNEX B – SUMMARY OF FINDINGS AND RECOMMENDATIONS FROM PREVIOUS DOD CIP VULNERABILITY ASSESSMENT STUDIES AND INVESTIGATIVE PROJECTS (1999-2003)

Project/Study	Problem Findings	Change Recommendations
Demonstration Projects – Tidewater Exercise (1999)	• No standard process to determine mission essential critical infrastructure assets • Inconsistent process to share assessment information • Current assessment methods generally do not generate desired CIP-relevant information	• DoD-developed guidelines for assessment information sharing of commercial asset information • DoD-developed analytical process to determine regional consequences in single asset failures • Synchronize established assessment methods with CIP analysis and assessment goals and requirements
Demonstration Projects – PACNORWEST (2000)	• Procedural inability to coordinate several assessment methods within a single assessment process to obtain appropriate CIP-relevant information • Duplicative assessment components within several assessment methodologies • All essential sector asset information was not identified at the start of the process • Current assessment methods are not all inclusive • Most current assessments are installation-focused and do not adequately address war-fighting command needs	• Establish specific analysis and assessment responsibilities to each assessing organizations • Establish assessment coordinating schedules and information-sharing procedures • Involve all appropriate Sector agencies in the analysis and assessment process to identify sector information needs • Include multiple assessment disciplines such as AT/FP, physical security, personnel security, information security, and operations security in the assessment process • Design assessments that are mission focused to ensure the effort provides usable information and identify asset interdependencies to war-fighting commanders. • Precede assessments with "mission-to-asset-to-site" analysis to link mission-dependent assets to the most appropriate assessment instrument.
Demonstration Projects – Malmstrom AFB (2000)	• Assessment methods are not synchronized (contain overlapping assessments) • Supporting commercial and DoD infrastructure assessments are not adequately coordinated • Insufficient on-site assessment information sharing.	• Coordinate multiple assessment methodologies to determine CIP-specific assessment objectives for each methodology • Conduct detailed pre-assessment coordination with DoD and commercial infrastructure asset owners to gain appropriate access and scheduling of assessment

Project/Study	Problem Findings	Change Recommendations
		activities. • Conduct routine joint assessment team and asset owner information sharing sessions concurrent with the assessment to ensure continued on-site cooperation, process feedback, and immediate remediation of some identified vulnerabilities.
Demonstration Projects –Rocky Mountain Corridor (2001)	• Existing assessment protocols did not permit automatic assessment information sharing without release from the installation or asset-owning commander, which restrains the access of CIP-relevant information • Protection of commercial vulnerability information is both a competitive and liability concern to commercial asset owners • Lack of an approved, consistent CIP analysis and assessment process leads to incomplete or inconsistent information gathering and reporting	• Revise assessment protocols to permit greater assessment information-sharing • Commercial vulnerability information must be protected through DoD procedural and national legislative action • Develop a consistent CIP analysis and assessment process for consistent information gathering and reporting
USPACOM/JPO-STC Appendix 16 Project	• No current DoD policy guidance on which to establish an approved and resourced vulnerability assessment program and standards. • Most current assessment organization procedures restrict scheduling and information release authority to installation & facility commanders • Multiple and uncoordinated and redundant assessment team visits • Current assessment final reports are neither timely nor formatted to convert assessment information to asset information databases. The inconsistencies result in long delays in obtaining important data (2-10 months) and expensive man-hour costs in collecting data from multi-page written reports and inserting the data into the command's asset database. • Current assessment organization	• Develop DoD assessment policy and guidance to achieve assessment effectiveness and authorization for required funding • Establish assessment procedures to give Combatant Commands responsibility to coordinate various assessment schedules – gives discipline to the scheduling process through scheduling synchronization, while tailoring the right assessment process to the proper infrastructure asset • Establish common CIP assessment processes to address: collection requirements based on the MER, asset tasks, asset functions, asset direct/indirect support organizations, and asset granularity (description, owner, location, loss consequence, vulnerabilities, and options for mitigation/response/reconstitution) • Change assessment final report procedures to ensure report is

Project/Study	Problem Findings	Change Recommendations
	procedures restrict assessment report distribution to the installation or facility requesting the assessment • Current assessment organization procedures constrain the number and types of concerned organizations that can be involved in the pre-assessment process	available to authorized recipients NLT 60 days after the assessment • Final assessment reports should be prepared with consistent data elements that can be entered into Combatant Command asset databases with minimum additional manpower requirements. • Change assessment procedures to permit Combatant Commanders as the principal assessment report recipient of all assessments within the command to permit information and data-sharing within the command, with the Defense Infrastructure Sector POCs, and placement into the command's asset database • Develop DoD-wide assessment procedures to permit pre-assessment coordination by the Combatant Commands with the participating assessment agencies to ensure that their assessments are tailored to the command's requirements. PACOM recommended that the coordination include team members from the selected assessed installation(s), the appropriate Service, and appropriate DI Sector representatives
OASD (C3I) Study Teams (IVA IPT) (VATWG) (2001-2003)	• Gaps and overlaps in assessment coverage of CIP-related issues exist within the existing (2001) DoD assessment methods: - Industrial base assets - Foreign assets - Commercial assets • Lacking specific DoD policy, the ability to resource CIP-related assessments remains limited • Lacking specific DoD policy, there is no standard assessment process to coordinate, integrate, execute assessments or share assessment results information • Lacking Specific DoD policy, there is not an effective means to access vulnerability assessment information by those responsible for DoD-wide risk management decisions	• The range of DoD assessments and the skill mix within the assessment organizations provide the capability to form an integrated DoD CIP assessment process ("leverage best practices") • Establish clear and comprehensive DoD policy to manage the CIP analysis and assessment processes: - Asset identification criteria - Asset prioritization - Asset assessment selection - Coordination & scheduling - Considerations for commercial, foreign, & industrial base assets - Considerations for information sharing (e.g., distribution, protection of proprietary data, classification) • Aggregation of vulnerability data requires a deliberate management of

Project/Study	Problem Findings	Change Recommendations
	• Existing assessments (2001) narrowly focus on installation vulnerabilities and do not assess infrastructures within mission context of the Combatant Commands	the requisite level of security classification • Establish a vulnerability assessment clearinghouse (catalog) to support information sharing and assessment scheduling • Designate a DoD agency as the Executive Agent for CIP vulnerability assessments • Establish a technical working group to develop common vulnerability assessment protocols for: - Standardize outputs - Information sharing - CIP risk management decisions - Off-site commercial assets using the JPO-STC IAP method - Core assessment process using the DTRA BSA method

ANNEX C - VULNERABILITY ASSESSMENT ANNOTATED BIBILOGRAPHY

Title & Agency	Summary
"*A CINC Mission Assurance Critical Infrastructure Protection Demonstration Project Work Plan*" (Draft) (OASD (C3I)) (2002)	A project plan to establish guidelines for the development of CIP VA demonstration projects to develop consistent procedures for the conduct of a CIP VA for mission critical infrastructure assets, both DoD and non-DoD. The plan outlines the process and identifies the types of information elements that should be developed during the demonstration project. This plan was not implemented because the concept of conducting these projects to support VA information gathering was replaced by the USPACOM Appendix 16 pilot project.
"*A Method to Assess the Vulnerability of U.S. Chemical Facilities*" (Dept of Justice, National Institute of Justice) (2002)	An assessment methodology developed in collaboration with the Dept of Energy's Sandia National Labs and the National Institute of Justice. Document addresses only physical security assessment methods.
"*American Petroleum Chemical Institute Security Vulnerability Assessment (SVA)*" (American Petroleum Chemical Institute) (1997)	This document is for the purpose of conducting security vulnerability assessment (SVA) to ID hazards, threats, and vulnerabilities facing a fixed facility handling hazardous material from malicious acts, and to evaluate the countermeasures to ensure the protection of the public, workers, national interests, the environment and the company. It ID the make-up of the team needed conduct these SVAs, and provide general guidelines for identifying critical assets, threats, etc.
"*Chemical Facilities Safeguards and Security Risk Assessment Methodology*" (Exxon/Mobile) (2000)	This document identifies the methodology adopted by the EM for conducing VA using risk scenario analysis. The Risk Assessment (RA) process consists of eight assessments and evaluation phases, and list measures under the Risk Assessment to make up a Risk Management Decision. Using a risk matrix, scenarios are assigned a qualitative risk rating based on the team's judgment of the scenario's severity of consequence and probability of occurrence. There is a system in place to screen and prioritize sites in order to develop a company priority list for facility further site evaluation.
"*A Standard DoD CIP Analysis and Assessment Process*" (JPO-STC) (2002)	A JPO-STC proposal for a standard DoD CIP process for conducting analysis and assessment activities. The proposal is based on three years of JPO-STC's A&A support to the CIP Component community. Provides a detailed description of each of the nine steps in the 9-Step A&A process.
CJCSI 3209.01, "*Critical Infrastructure Protection (CIP)*" (JS, J-5) (Draft) (2002)	Policies, definitions, and responsibilities for Joint Staff, Services, and Combatant Commands for their implementation of the DoD CIP program. Prepared in collaboration with DoDD 3020 (CIP) and share common terms and general guidance for implementation. Coordination of the draft suspended until approval of DoDD 3020 is given.
"*Critical Infrastructure Protection – Challenges in Securing Control Systems*"	Congressional testimony by the GAO that describes the cyber security risks associated with control systems, potential and reported cyber attacks against the systems, and the challenges and

Title & Agency	Summary
(General Accounting Office) (2003)	steps that must be taken to secure the systems.
"*Critical Infrastructure Protection Database Architecture Description and Needs (Version 1.1)*" (Draft) (JPO-STC) (2003)	Proposal and process document for the development of an overall database architecture for identified DoD CIP critical infrastructure assets. Describes the background of the problem, the purpose and rationale for an integrated CIP database methodology, and the process to develop the database.
"*Critical Infrastructure Protection Vulnerability Assessment Requirements Statement*" (OASD (C3I)) (2003)	A report following the VATWG Study that describes the capabilities, characteristics, tasks, and purpose of an integrated, DoD-wide, CIP vulnerability assessment program. Document describes the requirement and rationale to develop a CIP-specific assessment process that would integrate two or more current DTRA and JPO-STC assessments into a comprehensive CIP assessment.
"*Critical Infrastructure Protection Vulnerability Assessment Program Transition Document*" (Working Papers) (OUSD (S&IO)) (2003)	Follow-on document to the Requirements Statement cite in the reference entry immediately above. This document elaborates on the requirement statement to provide more details regarding the proposed integrated CIP assessment process for DoD. Details include protocols, source for the assessment's standards, post-assessment report organization, and preliminary timeline. Prepared during the period when CIP management was transferred from OASD (C3I) to OUSD (I), then to OASD (HD), this document was coordinated within the CIP Component community.
DoDD 2000.12, "*DoD Combating Terrorism Program*" (OASD (SO/LIC)), (1996)	Provides guidance to DoD personnel (military, civilians, & families) living or about to deploy to OCONUS locations. Provide knowledge on security awareness, risk assessment, protective measures, and guidance to DoD agencies for training and program implementation.
DoDI 2000.14, "*Combating Terrorism Program Procedures*" (OASD (SO/LIC)), (1994)	Document assigns DoD policies for the protection of DoD personnel (military, civilian, & families). Assigns responsibilities for AT training, threat awareness, and personnel protection. Designates high-risk locations and occupational positions.
DoDI 2000. 16, "*DoD Antiterrorism Standards*" (OASD (SO/LIC)), (2001)	This document provides guidance for security of personnel at domestic and overseas locations. It lists the standards as they apply to the Anti-Terrorism/Force Protection program, which includes: physical security assessment, vulnerability assessment, and operational readiness. It also provides a set of standards that each facility, base, etc. must follow in order to comply with this Instruction. Lastly, it refers to specific common criteria and minimum construction standards to mitigate antiterrorism vulnerabilities and terrorist threats.
DoDD 3020, "*Critical Infrastructure Protection (CIP) Program*" (Draft) (OASD (HD)/FP&E/CIP) (2003)	Policies, definitions, and responsibilities applicable to OSD, Military Departments, Defense Agencies, JCS, Combatant Commands for the implementation of the DoD CIP program. In coordination since 2002 and delayed until completion of DoD reorganization and designation of new CIP program management.
DoDI 3020, "*Implementation of the Critical Infrastructure Protection (CIP)* (Draft)	Instructions, procedures, definitions, and responsibilities applicable to OSD, Military Departments, Defense Agencies, JCS, Combatant Commands for the implementation of the DoD CIP

Title & Agency	Summary
(OASD (HD)/FP&E/CIP) (2003)	program. In coordination since 2002 and delayed until completion of DoD reorganization and designation of new CIP program management.
DoDD 3020.26, "*Continuity of Operations (COOP) Policy and Planning*" (OUSD (P)), (1995)	Policies, definitions, and responsibilities to ensure effective performance of critical DoD missions and continuation of mission-essential functions during emergencies.
DoDD 5160.54, "*Critical Asset Assurance Program (CAAP)*" (OUSD (P)), (1998)	DoD policies and responsibilities for the protection and assurance of DoD and non-DoD worldwide critical assets. Describes an integrated infrastructure vulnerability assessment and assurance program based on the analysis of identified critical assets using risk management principles
DoDD 5200.1 and 5200.1R, "*DoD Information Security Program*" (OASD (C3I)), (1997)	Policies, definitions, and responsibilities to safeguard DoD information systems, classification procedures, protection of classified materials, and guidelines for training programs
DoDD 5200.8, "*Security of DoD Installations and Resources*" (OUSD (P)), (1991)	Policy that directs installation commanders and tenant unit commanders to develop the necessary regulations for the protection of installations, sub-bases, and facilities.
DoD Handbook O-2000. 12H, "P*rotection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*" (OASD (SO/LIC)) (2000)	All-inclusive document on DoD policies and procedures for combating terrorism. Includes defining assets, vulnerability assessments, threat levels and warnings, reducing threats and public relations.
"*DoD Critical Infrastructure Protection Full Spectrum Vulnerability Assessment Program*" (Draft) (JPO-STC) (2003)	Current DoD concept proposal for a CIP vulnerability assessment process. Document takes a very similar approach to the issue as the former OUSD (I) transition Document (cited above). Document provides concept details including program development, requirements and standards, protocols, and training/certification requirements. This document is the start point for an extensive coordination process with CIP Component stakeholder organizations.
"*DoD FY 2002 CIP Annual Report*" (OASD (C3I)) (2003)	Detailed report listing and describing the major CIP activities conducted during FY 2002 by 33 CIP Component agencies. Each agency prepared a separate section that described their activities in 2002 and their 0bjectives for 2003 in six categories: CIP Program Overview, CIP Program Organization, FY 2002 CIP Program Operations, CIP Program Technologies, Tools, & Methodologies, and CIP Plans for FY 2003.
"DoD Critical Infrastructure Protection (CIP) Plan" (DASD (S&IO)) (1998)	Prepared in response to a PDD 63 requirement for DoD to develop a CIP program. Served as a guide to DoD Components in planning consideration to ensure that DoD infrastructures are available to support defense missions. Addresses tasks, responsibilities, procedures, and process to implement a CIP program. Document was not policy but guidance to the Military Departments, Defense Agencies, Joint Staff, and Combatant Commands.
"*DoD CIP Strategy*" (OASD (C3I)) (2003)	Published in April 2003, the CIP strategy is the most significant guidance document for the implementation of the DoD CIP program since the release of the DoD CIP Plan in 1998. The strategy identifies the CIP vision and implementation principles,

Title & Agency	Summary
	and a detailed description of each of the eleven areas of CIP strategy emphasis: CIP awareness, analysis and assessment, indications and warning, consequence management, investments, information architecture, research and development, outreach and education, defense industrial base, national-level interface, and international-level interface.
"*DoD Vulnerability Assessment Executive Summaries for DHS Transition Team*" (DTRA, Vulnerability Assessment Working Group) (2002)	This document provides an overview of the BSA assessment process. It outlines the BSA methodology, team sizes, length of assessments, cost, products, and how the BSA could be adapted to critical Federal, State or commercial sectors to protect critical infrastructure. This document also discusses some of the software tools used by the BSA team when conducting their assessments.
"*Functional Responsibilities Document*" (OASD (HD)/CIP) (2003)	OASD (HD) document that identified all of the assigned tasks for the new DoD CIP program office, the DPO-MA.
"*Georgia-Pacific Security Hazard Analysis (SHA)*" (Georgia-Pacific RR) (1996)	The analysis is a subset of the Facility Security Assessment (FSRA), aimed at specific exposures relative to hazardous materials. The analysis involves a five-step process of (1) defining the asset, (2) defining the threat, (3) conducting the VA, (4) selecting countermeasures & (5) implementing countermeasures. Assets are defined as vital, important and secondary, just as threats are defined as probable, possible and unlikely (catastrophic, moderate or insignificant). The vulnerability analysis is based on scenarios. The SHA teams use their employees who know the ends and outs of the organization, and they assume the roles of a criminal intent on attacking the organization. Each scenario is rated for plausibility, consequence, security and the organization's risk tolerance. Physical security measures play a major role in the document.
"*Homeland Security – Key Elements of a Risk Management Approach*" (General Accounting Office) (2001)	Testimony given to the US House of Representatives that give GAO recommended approach to manage the risk from terrorism directed against at Americans within the US. Recommendations based on GAO observations of US government counter-terrorism efforts prior to 11 September 2001
"*Integrated Vulnerability Assessment – Integrated Process Team Final Report*" (OASD (C3I) and Joint Staff J-5) (2001)	Report prepared at the end of a 12-month study of the 2001 uses of existing DoD vulnerability assessment for DoD CIP purposes. Recommendations advocated the development of DoD CIP VA policy, establishment of common protocols and standards, and the development of an assessment information sharing process. Report contains an assessment matrix listing 25 different characteristics for 22 different DoD assessment methods.
"*JSIVA Vulnerability Assessment Team Guidelines*" (DTRA), (2002)	Document used by DTRA's JSIVA assessment teams to guide team member assessment activities and to record observations from assessments. Document includes DoD standards from a wide range of directives, instructions, and Service regulations
Joint Pub 3-07.2, "*Joint Doctrine and Tactics for Dealing with Terrorism*" (Joint Staff) (1998)	Defines DoD roles under the Anti-terrorism programs. Provides an overview on terrorist tactics, organizations, types of targets, and other descriptive information. Addresses: legal guidance, installation and facility AT program guidance, crisis management procedures, and protective measures. The appendixes cover

Title & Agency	Summary
	vulnerability assessments, protective measures, physical security procedures and other aspects of the Anti-Terrorism Program.
"*Mission Assurance Asset Database (MAAD)*" (JPO-STC) (2002)	JPO-STC white paper that describes the MAAD database system that was JPO-STC-developed at the direction of the Joint Staff following the terrorist attacks on 11 September 2001. The paper briefly describes the purpose and functions of the database and how the database should be integrated into an overall CIP infrastructure database system.
"*National Strategy for Homeland Security*" (White House, Office of HLS), (2002)	Prepared as the foundation document from the Bush Administration to provide national guidance for homeland security. Broadly defines six critical mission areas for national attention, identifies critical infrastructure sectors, assigns departmental responsibilities, and provides guidance for implementation of a national program
"*OPORD 3020-03, Critical Infrastructure Protection*" (Draft) (J34, USPACOM) (2003)	Detailed description of the PACOM Appendix 16 development process, particularly the description of the command-developed analysis and assessment process. This process was co-developed with JPO-STC and was the pilot A&A process model for combatant commands.
"OSD/Joint Staff Vulnerability Assessment Technical Working Group Final Report" (OASD (C3I)) (2002)	The last analysis activity conducted by OASD (C3I) CIP Directorate to determine vulnerability assessment information sharing policy and establishment of a Office of Primary Responsibility (OPR) for developing standards and policy. The document provides general guidance to the subsequent resolution of these issues but did not make specific recommendations except to recommend the development of a VA information CD-ROM. JPO-STC produced this CD in 2003 (see reference above).
PDD 63, "*Critical Infrastructure Protection"* (White House) (1998)	Foundation document from the Clinton Administration for the current application of the national and DoD CIP program. Specifies the nature of the threat, requirements for infrastructure protection, identification of critical national infrastructures, assignment of departmental responsibilities, and generated the requirement for DoD to develop it CIP Plan in late 1998.
"*Protecting the Nation's Water Supply Since 9/11*" (Environmental Protection Agency) (2002)	A PowerPoint briefing on the need to develop water security standards to guard against terrorist attacks.
"R*ealignment of Critical Infrastructure Protection Oversight to the Assistant Secretary of Defense for Homeland Defense*" (DepSecDef) (2003)	Authorization document that directed the change of DoD CIP management and responsibility from OUSD (I) to OASD (HS). Gives specific responsibilities to the staff of the new DoD CIP Directorate. Addresses the office responsibility to develop a CIP-specific VA program for DoD.
"*Rocky Mountain Corridor Analysis and Assessment Process Report*" (OASD (C3I)) (2001)	Project summary report that describes the largest and final of the four-project Demonstration Projects. Describes the project's methodology and summarized the findings and recommendations.
"*Site Security Guidelines for the U.S. Chemical Industry*" (American Chemistry Council), (2001)	A document tool to assist plant managers, operations managers, and others in management to secure their resources based on risk. Identifies possible vulnerable assets, security measures, contains a sample site security analysis, and outlines a six-step process for

Title & Agency	Summary
	vulnerability assessment.
"*The U.S. EPA regional Vulnerability Assessment Program: A Research Strategy for 2001-2006*" (Environmental Protection Agency (2000)	Presents the EPA research strategy for the ReVA program. Provides guidance for prioritizing research projects necessary to conduct regional vulnerability assessments, development of research plans, and overall assessment research strategies.
"*Vulnerability Assessment and Survey Methodology*" (U.S. Department of Energy" Office of Energy Assurance)	The vulnerability assessment and survey methodology from the U.S. department of energy provides guidance to the U.S. energy industry (electric, power, oil, and natural gas) on protecting the nation's energy infrastructures.
"*Vulnerability Assessment Catalog*" (CD-ROM) (JPO-STC) (2003)	CD-ROM developed by JPO-STC in response to a recommendation from the DoD VATWG team final report for a vulnerability assessment catalog of previous DoD assessment activities. The catalog identifies 844 assessment activities conducted by 9 assessment agencies. The catalog is an on-going activity that JPO-STC will update on an annual basis. The current catalog covers the years 1998 to 2002.